日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日
Date of Application: ２００２年 ３月 ５日

出 願 番 号
Application Number: 特願２００２－０５９１７９

[ST.10/C]: [ＪＰ２００２－０５９１７９]

出 願 人
Applicant(s):

三洋電機株式会社
シャープ株式会社
日本ビクター株式会社
パイオニア株式会社
株式会社日立製作所
フェニックステクノロジーズ株式会社
富士通株式会社

２００３年 ４月 ８日

特 許 庁 長 官
Commissioner,
Japan Patent Office 太田信一郎

出証番号 出証特２００３－３０２４２７９

【書類名】　特許願

【整理番号】　1020002

【提出日】　平成14年 3月 5日

【あて先】　特許庁長官殿

【国際特許分類】　H04M 11/08

【発明者】

【住所又は居所】　大阪府守口市京阪本通２丁目５番５号　三洋電機株式会社内

【氏名】　堀　吉宏

【発明者】

【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号　シャープ株式会社内

【氏名】　大野　良治

【発明者】

【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地　日本ビクター株式会社内

【氏名】　大石　剛士

【発明者】

【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内

【氏名】　戸崎　明宏

【発明者】

【住所又は居所】　埼玉県所沢市花園４丁目２６１０番地　パイオニア株式会社　所沢工場内

【氏名】　多田　謙一郎

【発明者】

【住所又は居所】　神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所　システム開発研究所内

【氏名】　平井　達哉

【発明者】
【住所又は居所】　東京都新宿区新宿４－２－１８　新宿光風ビル６Ｆ　フェニックステクノロジーズ株式会社内
【氏名】　津留　雅文
【発明者】
【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
【氏名】　長谷部　高行
【特許出願人】
【識別番号】　000001889
【住所又は居所】　大阪府守口市京阪本通２丁目５番５号
【氏名又は名称】　三洋電機株式会社
【特許出願人】
【識別番号】　000005049
【住所又は居所】　大阪府大阪市阿倍野区長池町２２番２２号
【氏名又は名称】　シャープ株式会社
【特許出願人】
【識別番号】　000004329
【住所又は居所】　神奈川県横浜市神奈川区守屋町３丁目１２番地
【氏名又は名称】　日本ビクター株式会社
【特許出願人】
【識別番号】　000005016
【住所又は居所】　東京都目黒区目黒１丁目４番１号
【氏名又は名称】　パイオニア株式会社
【特許出願人】
【識別番号】　000005108
【住所又は居所】　東京都千代田区神田駿河台４丁目６番地
【氏名又は名称】　株式会社日立製作所

【特許出願人】
【識別番号】 300017636
【住所又は居所】 東京都新宿区新宿４－２－１８　新宿光風ビル６Ｆ
【氏名又は名称】 フェニックステクノロジーズ株式会社
【特許出願人】
【識別番号】 000005223
【住所又は居所】 神奈川県川崎市中原区上小田中４丁目１番１号
【氏名又は名称】 富士通株式会社
【代理人】
【識別番号】 100064746
【弁理士】
【氏名又は名称】 深見　久郎
【選任した代理人】
【識別番号】 100085132
【弁理士】
【氏名又は名称】 森田　俊雄
【選任した代理人】
【識別番号】 100091409
【弁理士】
【氏名又は名称】 伊藤　英彦
【選任した代理人】
【識別番号】 100096781
【弁理士】
【氏名又は名称】 堀井　豊
【手数料の表示】
【予納台帳番号】 008693
【納付金額】 21,000円
【提出物件の目録】
【物件名】 明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　データ記憶装置

【特許請求の範囲】

【請求項１】　機密データを保護するための所定の入出力手順に従って前記機密データの入出力を行ない、かつ、前記機密データを記憶するデータ記憶装置であって、

外部とデータのやり取りを行なうインターフェース手段と、

前記機密データを記憶する第１の記憶手段と、

前記所定の入出力手順に従った前記機密データの入出力に関するログ情報と入出力の対象となる前記機密データの前記第１の記憶手段における記憶位置を示すアドレスとを記憶する第２の記憶手段とを備えるデータ記憶装置。

【請求項２】　前記機密データの入出力を制御する制御手段をさらに備え、

前記ログ情報は、

入出力の対象となる前記機密データを識別する識別コードと、

入出力の対象となる前記機密データの前記第１の記憶手段における記憶状態を示す第１のステータスとを含み、

前記制御手段は、前記所定の入出力手順に従って、入出力の対象となる前記機密データの前記識別コードと前記アドレスとを前記インターフェース手段を介して受取ると前記第２の記憶手段に記憶し、前記インターフェース手段を介して受ける外部からの要求に応じて、前記第２の記憶手段に記憶された前記識別コードと前記アドレスとに基づいて前記第１の記憶手段における前記機密データの記憶状態を確認し、前記記憶状態に基づいて前記第１のステータスを更新する、請求項１に記載のデータ記憶装置。

【請求項３】　前記ログ情報は、入出力の対象となった前記機密データの入出力における前記所定の入出力手順の進行状態を記録する第２のステータスをさらに含み、

前記制御手段は、前記所定の入出力手順の進行に応じて前記第２のステータスを更新する、請求項２に記載のデータ記憶装置。

【請求項４】　前記ログ情報は、前記所定の入出力手順を特定する手順特定

情報をさらに含み、

前記制御手段は、前記手順特定情報を新たに取得するごとに前記手順特定情報を更新する、請求項２または請求項３に記載のデータ記憶装置。

【請求項５】　前記機密データは、その機密データに固有の前記識別コードを含み、

前記制御手段は、前記第１の記憶手段における前記機密データの記憶状態を確認するとき、前記アドレスによって特定される前記第１の記憶手段上の記憶位置に記憶されている前記機密データに含まれる前記識別コードによって前記機密データを特定する、請求項２から請求項４のいずれか１項に記載のデータ記憶装置。

【請求項６】　前記機密データを前記インターフェース手段を介して受取って前記第１の記憶手段に記憶する入力手順において、

前記制御手段は、前記受取った機密データに含まれる識別コードと前記ログ情報に含まれる識別コードとが一致しないとき、前記機密データを前記第１の記憶手段に記憶することなく、前記入力手順を中止する、請求項５に記載のデータ記憶装置。

【請求項７】　前記第１の記憶手段に記憶された前記機密データを前記インターフェース手段を介して出力する出力手順において、

前記制御手段は、前記アドレスによって特定される前記第１の記憶手段上の記憶位置に記憶されている前記機密データに含まれる識別コードと前記ログ情報に含まれる識別コードとが一致しないとき、前記機密データの出力を行なうことなく、前記出力手順を中止する、請求項５または請求項６に記載のデータ記憶装置。

【請求項８】　前記ログ情報に対する署名データを生成し、前記生成した署名データを前記ログ情報に添付した署名付きログ情報を生成する署名手段をさらに備え、

前記機密データを前記インターフェース手段を介して受取って前記第１の記憶手段に記憶する入力手順が中断した場合、中断した前記入力手順を再開する再入力手順において、

前記制御手段は、前記署名手段によって生成された前記署名付きログ情報を前記インターフェース手段を介して出力する、請求項２から請求項７のいずれか１項に記載のデータ記憶装置。

【請求項９】　前記インターフェース手段を介して前記機密データの提供先から受取った、前記提供先のもう１つのログ情報に対する署名データが前記もう１つのログ情報に添付されたもう１つの署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、

前記第１の記憶手段に記憶された前記機密データを前記インターフェース手段を介して出力する出力手順が中断した場合、中断した前記出力手順を再開する再出力手順において、

前記ログ認証手段は、前記中断した出力手順における前記機密データの提供先から受取った前記もう１つの署名付きログ情報の正当性を検証し、

前記制御手段は、前記もう１つの署名付きログ情報が正当でないと判断されたとき、または、前記もう１つの署名付きログ情報が正当であると認証され、かつ、前記もう１つの署名付きログ情報と前記第２の記憶手段に記憶される前記ログ情報とに基づいて前記出力手順が中断していないと判断したとき、前記再出力手順を中止する、請求項８に記載のデータ記憶装置。

【請求項１０】　前記機密データの提供元に対して出力する証明書を保持する証明書保持手段をさらに備え、

前記制御手段は、前記機密データを前記インターフェース手段を介して受取って前記第１の記憶手段に記憶する入力手順を開始するに際し、前記インターフェース手段を介して受取った前記証明書の出力要求に応じて前記証明書を前記インターフェース手段を介して出力し、前記提供元において前記証明書が認証されると、前記提供元から前記インターフェース手段を介して前記機密データを受取る、請求項４に記載のデータ記憶装置。

【請求項１１】　前記証明書は、当該データ記憶装置に対応した公開鍵を含み、

前記公開鍵により暗号化されたデータを復号するための秘密鍵を保持する秘密鍵保持手段と、

前記公開鍵により暗号化されたデータを前記秘密鍵により復号する第１の復号処理手段と、

前記機密データを入出力する前記所定の入出力手順において、前記所定の入出力手順ごとに固有の第１のセッション鍵を生成するセッション鍵生成手段と、

前記提供元において生成された第２のセッション鍵によりデータを暗号化する暗号処理手段と、

前記第１のセッション鍵により暗号化されたデータを復号する第２の復号処理手段とをさらに備え、

前記入力手順において、

前記セッション鍵生成手段は、前記第１のセッション鍵を生成し、

前記第１の復号処理手段は、前記公開鍵により暗号化された前記第２のセッション鍵を前記秘密鍵により復号し、

前記暗号処理手段は、前記第１の復号処理手段から受けた前記第２のセッション鍵により前記第１のセッション鍵を暗号化し、

前記第２の復号処理手段は、前記第１のセッション鍵により暗号化された前記機密データを前記第１のセッション鍵により復号し、

前記制御手段は、前記提供元から前記インターフェース手段を介して受取った前記公開鍵によって暗号化された前記第２のセッション鍵を前記第１の復号処理手段に与え、前記第２のセッション鍵により暗号化された前記第１のセッション鍵を前記インターフェース手段を介して前記提供元に対して提供するために出力し、前記提供元から前記インターフェース手段を介して受取った前記第１のセッション鍵により暗号化された前記機密データを前記第２の復号処理手段に与え、復号された前記機密データを前記アドレスによって特定される前記第１の記憶手段上の記憶位置に記憶する、請求項１０に記載のデータ記憶装置。

【請求項１２】　前記手順特定情報は、前記入力手順を特定する前記第１のセッション鍵であり、

前記制御手段は、前記セッション鍵生成手段によって前記第１のセッション鍵が生成されるごとに前記手順特定情報を更新する、請求項１１に記載のデータ記憶装置。

【請求項１３】　前記第１の復号処理手段から受けた前記第２のセッション鍵によって認証可能な前記ログ情報に対する署名データを生成し、前記生成した署名データを前記ログ情報に添付した署名付きログ情報を生成する署名手段をさらに備え、

前記入力手順が中断した場合に前記入力手順を再開する再入力手順において、

前記第１の復号処理手段は、新たに前記提供元から前記インターフェース手段を介して受取った前記公開鍵によって暗号化された前記第２のセッション鍵を復号し、

前記署名手段は、前記第２の記憶手段に記憶される前記第１のステータスが更新された後、新たに受取られた前記第２のセッション鍵によって前記署名付きログ情報を生成し、

前記制御手段は、新たに前記提供元から前記インターフェース手段を介して受取った前記公開鍵によって暗号化された前記第２のセッション鍵を前記第１の復号処理手段に与え、前記第１のステータスを更新し、前記署名手段によって生成された前記署名付きログ情報を前記インターフェース手段を介して前記提供元に対して提供するために出力する、請求項１１または請求項１２に記載のデータ記憶装置。

【請求項１４】　前記機密データは、その機密データに固有の前記識別コードを含み、

前記制御手段は、前記第１の記憶手段における前記機密データの記憶状態を確認するとき、前記アドレスによって特定される前記第１の記憶手段上の記憶位置に記憶されている前記機密データに含まれる前記識別コードによって前記機密データを特定する、請求項１０から請求項１３のいずれか１項に記載のデータ記憶装置。

【請求項１５】　前記制御手段は、前記受取った機密データに含まれる識別コードと前記ログ情報に含まれる識別コードとが一致しないとき、前記機密データの前記第１の記憶手段への記憶を中止する、請求項１４に記載のデータ記憶装置。

【請求項１６】　前記第１の記憶手段に記憶された前記機密データを提供す

る提供先から受取った、前記提供先のもう１つの証明書の正当性を検証して認証する認証手段をさらに備え、

前記機密データを前記インターフェース手段を介して出力する出力手順において、

前記認証手段は、前記提供先から受取った前記もう１つの証明書を検証し、

前記制御手段は、前記提供先から前記インターフェース手段を介して受取った前記もう１つの証明書を前記認証手段に与え、前記認証手段によって前記もう１つの証明書が認証されないとき、前記出力手順を中止する、請求項１０に記載のデータ記憶装置。

【請求項１７】　前記第１の記憶手段に記憶された前記機密データを提供する提供先から受取った、前記提供先のもう１つの証明書の正当性を検証して認証する認証手段と、

前記もう１つの証明書に含まれる前記提供先に対応した公開鍵によってデータを暗号化するもう１つの暗号処理手段とをさらに備え、

前記機密データを前記インターフェース手段を介して出力する出力手順において、

前記認証手段は、前記提供先から受取った前記もう１つの証明書を検証し、

前記セッション鍵生成手段は、第３のセッション鍵をさらに生成し、

前記もう１つの暗号処理手段は、前記提供先に対応した公開鍵により前記第３のセッション鍵を暗号化し、

前記第２の復号処理手段は、前記第３のセッション鍵により暗号化された前記提供先において生成された第４のセッション鍵を前記第３のセッション鍵によりさらに復号し、

前記暗号処理手段は、前記第２の復号処理手段から受けた前記第４のセッション鍵により前記機密データをさらに暗号化し、

前記制御手段は、前記提供先から前記インターフェース手段を介して受取った前記もう１つの証明書を前記認証手段に与え、前記認証手段によって前記もう１つの証明書が認証されたとき、前記もう１つの証明書に含まれる前記提供先に対応した公開鍵を前記もう１つの暗号処理手段に与え、前記提供先に対応した公開

鍵により暗号化された前記第３のセッション鍵を前記インターフェース手段を介して前記提供先に対して提供するために出力し、前記提供先から前記インターフェース手段を介して受取った前記第３のセッション鍵により暗号化された前記第４のセッション鍵を前記第２の復号処理手段に与え、前記アドレスによって特定される前記第１の記憶手段上の記憶位置に記憶される前記機密データを取得して前記暗号処理手段に与え、前記第４のセッション鍵により暗号化された前記機密データを前記インターフェース手段を介して前記提供先に対して提供するために出力する、請求項１１から請求項１３のいずれか１項に記載のデータ記憶装置。

【請求項１８】　前記手順特定情報は、前記出力手順を特定する前記第４のセッション鍵であり、

前記制御手段は、前記第２の復号処理手段によって前記第３のセッション鍵により暗号化された前記第４のセッション鍵が復号されるごとに前記手順特定情報を更新する、請求項１７に記載のデータ記憶装置。

【請求項１９】　前記機密データは、その機密データに固有の前記識別コードを含み、

前記制御手段は、前記アドレスによって特定される前記第１の記憶手段上の記憶位置に記憶されている前記機密データに含まれる前記識別コードと前記ログ情報に含まれる識別コードとが一致しないとき、前記機密データの出力を行なうことなく、前記出力手順を中止する、請求項１６から請求項１８のいずれか１項に記載のデータ記憶装置。

【請求項２０】　前記インターフェース手段を介して前記機密データの提供先から受取った、前記提供先のもう１つのログ情報に対する署名データが前記もう１つのログ情報に添付された署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、

前記第１の記憶手段に記憶された前記機密データを前記インターフェース手段を介して出力する出力手順が中断した場合、中断した前記出力手順を再開する再出力手順において、

前記ログ認証手段は、前記中断した出力手順における前記機密データの提供先から受取った前記署名付きログ情報の正当性を検証し、

前記制御手段は、前記署名付きログ情報が正当でないと判断されたとき、または、前記署名付きログ情報が正当であると認証され、かつ、前記署名付きログ情報と当該データ記憶装置の前記第２の記憶手段に記憶される前記ログ情報とに基づいて前記出力手順が中断していないと判断したとき、前記再出力手順を中止する、請求項１６に記載のデータ記憶装置。

【請求項２１】　前記インターフェース手段を介して前記機密データの提供先から受取った、前記第４のセッション鍵によって前記提供先のもう１つのログ情報に署名されたもう１つの署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、

前記第１の記憶手段に記憶された前記機密データを前記インターフェース手段を介して出力する出力手順が中断した場合、中断した前記出力手順を再開する再出力手順において、

前記ログ認証手段は、前記中断した出力手順における前記機密データの提供先から受取った前記もう１つの署名付きログ情報の正当性を検証し、

前記制御手段は、前記もう１つの署名付きログ情報が正当でないと判断されたとき、または、前記もう１つの署名付きログ情報が正当であると認証され、かつ、前記もう１つの署名付きログ情報と当該データ記憶装置の前記第２の記憶手段に記憶される前記ログ情報とに基づいて前記出力手順が中断していないと判断したとき、前記再出力手順を中止する、請求項１７または請求項１８に記載のデータ記憶装置。

【請求項２２】　前記機密データは、暗号化されたコンテンツデータを復号して利用するための復号鍵であって、

前記暗号化されたコンテンツデータを記憶するための第３の記憶手段をさらに備える、請求項１から請求項２１のいずれか１項に記載のデータ記憶装置。

【請求項２３】　前記第３の記憶手段は、ハードディスクである、請求項２２に記載のデータ記憶装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

この発明は、デジタルデータ化されたコンテンツデータに対する著作権保護を可能とするデータ配信システムにおけるデータ記憶装置に関し、特に、コンテンツデータを暗号化した暗号化コンテンツデータの再生に際して必要とされるライセンス（復号鍵および利用規則）を安全に入出力し、かつ、多数のライセンスを記憶することができ、さらには、保護を必要とする機密データを安全に入出力し、かつ、機密データの入出力の中断から安全に入出力を再開できるデータ記憶装置に関する。

【０００２】

【従来の技術】

近年、インターネット等のデジタル情報通信網等の進歩により、個人端末から各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

【０００３】

このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

【０００４】

したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツが伝送される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

【０００５】

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツの配信を行なうことができないとすると、基本的には、コンテンツデータの複製に際して一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

【０００６】

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデ

ータを記録した記録媒体を例にとって考えてみると、通常販売されている音楽データを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して補償金として支払うことになっている。

【０００７】

しかも、ＣＤからＭＤへ音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

【０００８】

このような事情からも、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

【０００９】

同様に、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

【００１０】

そこで、デジタル情報通信網を介したデータ配信システムとして、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバから携帯電話機などの端末装置に装着されたデータ記憶装置としてのメモリカードに対して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書とを暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、認証された証明書を配信サーバが受信したことを確認した上で、暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのコンテンツ鍵とをメ

モリカードに対して送信する。そして、暗号化コンテンツデータやコンテンツ鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッション鍵を発生させ、その発生させたセッション鍵によって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

【００１１】

最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッション鍵によって暗号化したライセンスと、暗号化コンテンツデータとをメモリカードへ送信する。そして、メモリカードは、受信したコンテンツ鍵と暗号化コンテンツデータとをメモリに記憶する。

【００１２】

そして、ユーザは、メモリカードに記憶した暗号化コンテンツデータを再生するときは、メモリカードを専用の再生回路を備えた再生端末に接続し、その暗号化コンテンツデータを再生して楽しむことができる。

【００１３】

このようなシステムにおいて、コンテンツ供給者あるいは著作権者によって暗号化コンテンツデータの再生や複製に関する利用方法が指示できるように利用規則を定め、この利用規則をコンテンツ鍵とともに配信し、各機器が利用規則に従って処理を行なうことができるようになっている。

【００１４】

利用規則には、メモリカード間のライセンスの複製・移動に関する規則、再生回数の制限などのコンテンツ鍵をメモリカードから出力する場合の規制や、再生されたコンテンツの取扱いに関する規則が規定されている。

【００１５】

【発明が解決しようとする課題】

上述したようなデータ配信システムにおいては、暗号化コンテンツデータと、暗号化コンテンツデータの復号および利用に関するライセンスとが、配信サーバとデータ記憶装置との間や、あるいはデータ記憶装置と再生端末との間などで送受信される。ここで、ライセンスとは、暗号化コンテンツデータを復号するためのコンテンツ鍵や、コンテンツに対するライセンスを特定するためのライセンス

ＩＤ、あるいは上述したコンテンツの利用規則などを総称するものである。そして、このライセンスこそが著作権を保護する目的からセキュリティに十分配慮して送受信されるべきものである。

【００１６】

ここで、ライセンスを装置間で送受信する際に、通常の送受信処理中であれば、送信側と受信側とにおいて送受信を行なっているライセンスを互いに認識し、ライセンスは両装置の間を問題なく送受信されるが、ライセンスの送受信中にいずれかの装置あるいは通信路において異常（たとえば、装置の電源の遮断など）が発生すると、送受信中のライセンスが消失してしまうことがある。

【００１７】

たとえば、データ記憶装置間でライセンスの送受信を行なう場合、利用規則によってライセンスの複製が許可されているフリーなコンテンツを除いては、著作権保護の観点から、送信側のデータ記憶装置および受信側のデータ記憶装置の両装置において同時に同一のライセンスが利用可能な状態で記憶できない構成となっている。すなわち、送信側のデータ記憶装置に記憶されているライセンスは、受信側のデータ記憶装置に対してライセンスを出力すると同時に利用できないものとなる必要がある。このような場合、一時的にではあるが、両データ記憶装置のいずれにも利用できるライセンスが記憶されていない状態が発生する。このような場合において、異常が発生して送受信処理が中断すると、送信中のライセンスが消失してしまうのである。配信サーバからライセンスを受信する場合においても、同様にライセンスの消失の危険性がある。したがって、ライセンスの送受信が中断した場合に、中断した送受信処理およびライセンスを特定し、特定したライセンスの記憶状態を把握したうえで、ライセンスの消失が発生した場合には、消失したライセンスの再送信処理をいかに適切に行なうかが重要になってくる。そして、データ記憶装置には、送受信中であった送受信処理とライセンスとを再度特定するための情報を効率的に記録しておく必要がある。

【００１８】

一方、近年、そして今後さらなる飛躍的進歩が確実視されるＩＴ技術の進展に伴う情報量の増大、情報のマルチメディア化、通信技術の高度化、また、メモリ

技術の進展に伴うデータ記憶装置の大容量化などとあいまって、上述したデータ配信システムにおけるデータ記憶装置には、多種多様、かつ、相当数のコンテンツデータが記憶されるものと予想される。

【００１９】

この場合、大容量のデータ記憶装置において相当数のコンテンツデータを記憶し、それに伴って各々のコンテンツデータに対応するライセンスを保持している場合において、上述したデータ配信システムにおいてライセンスの送受信処理中に異常が発生したときに、送受信中のライセンスを相当数記憶されたライセンスの中から再度特定することは、記憶されるライセンスの数が増えるほど、その検索に時間がかかることになる。

【００２０】

従来のシステムにおいては、このような場合、全てのライセンスを逐一検索して特定するしかなく、検索に要する処理時間が問題とされていた。

【００２１】

そこで、この発明は、かかる課題を解決するためになされたものであり、その目的は、相当数記憶されたライセンスの中から送受信処理中のライセンスを迅速に特定でき、特にライセンスの送受信処理中に異常が発生したときに、ライセンスの保護と再処理の高速化とを両立するデータ記憶装置を提供することである。

【００２２】

【課題を解決するための手段】

この発明によれば、データ記憶装置は、機密データを保護するための所定の入出力手順に従って機密データの入出力を行ない、かつ、機密データを記憶するデータ記憶装置であって、外部とデータのやり取りを行なうインターフェース手段と、機密データを記憶する第１の記憶手段と、所定の入出力手順に従った機密データの入出力に関するログ情報と入出力の対象となる機密データの第１の記憶手段における記憶位置を示すアドレスとを記憶する第２の記憶手段とを備える。

【００２３】

好ましくは、データ記憶装置は、機密データの入出力を制御する制御手段をさらに備え、ログ情報は、入出力の対象となる機密データを識別する識別コードと

、入出力の対象となる機密データの第１の記憶手段における記憶状態を示す第１のステータスとを含み、制御手段は、所定の入出力手順に従って、入出力の対象となる機密データの識別コードとアドレスとをインターフェース手段を介して受取ると第２の記憶手段に記憶し、インターフェース手段を介して受ける外部からの要求に応じて、第２の記憶手段に記憶された識別コードとアドレスとに基づいて第１の記憶手段における機密データの記憶状態を確認し、記憶状態に基づいて第１のステータスを更新する。

【００２４】

好ましくは、ログ情報は、入出力の対象となった機密データの入出力における所定の入出力手順の進行状態を記録する第２のステータスをさらに含み、制御手段は、所定の入出力手順の進行に応じて第２のステータスを更新する。

【００２５】

好ましくは、ログ情報は、所定の入出力手順を特定する手順特定情報をさらに含み、制御手段は、手順特定情報を新たに取得するごとに手順特定情報を更新する。

【００２６】

好ましくは、機密データは、その機密データに固有の識別コードを含み、制御手段は、第１の記憶手段における機密データの記憶状態を確認するとき、アドレスによって特定される第１の記憶手段上の記憶位置に記憶されている機密データに含まれる識別コードによって機密データを特定する。

【００２７】

好ましくは、機密データをインターフェース手段を介して受取って第１の記憶手段に記憶する入力手順において、制御手段は、受取った機密データに含まれる識別コードとログ情報に含まれる識別コードとが一致しないとき、機密データを第１の記憶手段に記憶することなく、入力手順を中止する。

【００２８】

好ましくは、第１の記憶手段に記憶された機密データをインターフェース手段を介して出力する出力手順において、制御手段は、アドレスによって特定される第１の記憶手段上の記憶位置に記憶されている機密データに含まれる識別コード

とログ情報に含まれる識別コードとが一致しないとき、機密データの出力を行なうことなく、出力手順を中止する。

【００２９】

好ましくは、データ記憶装置は、ログ情報に対する署名データを生成し、生成した署名データをログ情報に添付した署名付きログ情報を生成する署名手段をさらに備え、機密データをインターフェース手段を介して受取って第１の記憶手段に記憶する入力手順が中断した場合、中断した入力手順を再開する再入力手順において、制御手段は、署名手段によって生成された署名付きログ情報をインターフェース手段を介して出力する。

【００３０】

好ましくは、データ記憶装置は、インターフェース手段を介して機密データの提供先から受取った、提供先のログ情報に対する署名データが提供先のログ情報に添付されたもう１つの署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、第１の記憶手段に記憶された機密データをインターフェース手段を介して出力する出力手順が中断した場合、中断した出力手順を再開する再出力手順において、ログ認証手段は、中断した出力手順における機密データの提供先から受取ったもう１つの署名付きログ情報の正当性を検証し、制御手段は、もう１つの署名付きログ情報が正当でないと判断されたとき、または、もう１つの署名付きログ情報が正当であると認証され、かつ、もう１つの署名付きログ情報と第２の記憶手段に記憶される当該データ記憶装置のログ情報とに基づいて出力手順が中断していないと判断したとき、再出力手順を中止する。

【００３１】

好ましくは、データ記憶装置は、機密データの提供元に対して出力する証明書を保持する証明書保持手段をさらに備え、制御手段は、機密データをインターフェース手段を介して受取って第１の記憶手段に記憶する入力手順を開始するに際し、インターフェース手段を介して受取った証明書の出力要求に応じて証明書をインターフェース手段を介して出力し、提供元において証明書が認証されると、提供元からインターフェース手段を介して機密データを受取る。

【００３２】

好ましくは、証明書は、当該データ記憶装置に対応した公開鍵を含み、公開鍵により暗号化されたデータを復号するための秘密鍵を保持する秘密鍵保持手段と、公開鍵により暗号化されたデータを秘密鍵により復号する第１の復号処理手段と、機密データを入出力する所定の入出力手順において、所定の入出力手順ごとに固有の第１のセッション鍵を生成するセッション鍵生成手段と、提供元において生成された第２のセッション鍵によりデータを暗号化する暗号処理手段と、第１のセッション鍵により暗号化されたデータを復号する第２の復号処理手段とをさらに備え、入力手順において、セッション鍵生成手段は、第１のセッション鍵を生成し、第１の復号処理手段は、公開鍵により暗号化された第２のセッション鍵を秘密鍵により復号し、暗号処理手段は、第１の復号処理手段から受けた第２のセッション鍵により第１のセッション鍵を暗号化し、第２の復号処理手段は、第１のセッション鍵により暗号化された機密データを第１のセッション鍵により復号し、制御手段は、提供元からインターフェース手段を介して受取った公開鍵によって暗号化された第２のセッション鍵を第１の復号処理手段に与え、第２のセッション鍵により暗号化された第１のセッション鍵をインターフェース手段を介して提供元に対して提供するために出力し、提供元からインターフェース手段を介して受取った第１のセッション鍵により暗号化された機密データを第２の復号処理手段に与え、復号された機密データをアドレスによって特定される第１の記憶手段上の記憶位置に記憶する。

【００３３】

好ましくは、手順特定情報は、入力手順を特定する第１のセッション鍵であり、制御手段は、セッション鍵生成手段によって第１のセッション鍵が生成されるごとに手順特定情報を更新する。

【００３４】

好ましくは、データ記憶装置は、第１の復号処理手段から受けた第２のセッション鍵によって認証可能なログ情報に対する署名データを生成し、生成した署名データをログ情報に添付した署名付きログ情報を生成する署名手段をさらに備え、入力手順が中断した場合に入力手順を再開する再入力手順において、第１の復号処理手段は、新たに提供元からインターフェース手段を介して受取った公開鍵

によって暗号化された第２のセッション鍵を復号し、署名手段は、第２の記憶手段に記憶される第１のステータスが更新された後、新たに受取られた第２のセッション鍵によって署名付きログ情報を生成し、制御手段は、新たに提供元からインターフェース手段を介して受取った公開鍵によって暗号化された第２のセッション鍵を第１の復号処理手段に与え、第１のステータスを更新し、署名手段によって生成された署名付きログ情報をインターフェース手段を介して提供元に対して提供するために出力する。

【００３５】

好ましくは、機密データは、その機密データに固有の識別コードを含み、制御手段は、第１の記憶手段における機密データの記憶状態を確認するとき、アドレスによって特定される第１の記憶手段上の記憶位置に記憶されている機密データに含まれる識別コードによって機密データを特定する。

【００３６】

好ましくは、制御手段は、受取った機密データに含まれる識別コードとログ情報に含まれる識別コードとが一致しないとき、機密データの第１の記憶手段への記憶を中止する。

【００３７】

好ましくは、データ記憶装置は、第１の記憶手段に記憶された機密データを提供する提供先から受取った、提供先のもう１つの証明書の正当性を検証して認証する認証手段をさらに備え、機密データをインターフェース手段を介して出力する出力手順において、認証手段は、提供先から受取ったもう１つの証明書を検証し、制御手段は、提供先からインターフェース手段を介して受取ったもう１つの証明書を認証手段に与え、認証手段によってもう１つの証明書が認証されないとき、出力手順を中止する。

【００３８】

好ましくは、データ記憶装置は、第１の記憶手段に記憶された機密データを提供する提供先から受取った、提供先のもう１つの証明書の正当性を検証して認証する認証手段と、もう１つの証明書に含まれる提供先に対応した公開鍵によってデータを暗号化するもう１つの暗号処理手段とをさらに備え、機密データをイン

ターフェース手段を介して出力する出力手順において、認証手段は、提供先から受取ったもう１つの証明書を検証し、セッション鍵生成手段は、第３のセッション鍵をさらに生成し、もう１つの暗号処理手段は、提供先に対応した公開鍵により第３のセッション鍵を暗号化し、第２の復号処理手段は、第３のセッション鍵により暗号化された提供先において生成された第４のセッション鍵を第３のセッション鍵によりさらに復号し、暗号処理手段は、第２の復号処理手段から受けた第４のセッション鍵により機密データをさらに暗号化し、制御手段は、提供先からインターフェース手段を介して受取ったもう１つの証明書を認証手段に与え、認証手段によってもう１つの証明書が認証されたとき、もう１つの証明書に含まれる提供先に対応した公開鍵をもう１つの暗号処理手段に与え、提供先に対応した公開鍵により暗号化された第３のセッション鍵をインターフェース手段を介して提供先に対して提供するために出力し、提供先からインターフェース手段を介して受取った第３のセッション鍵により暗号化された第４のセッション鍵を第２の復号処理手段に与え、アドレスによって特定される第１の記憶手段上の記憶位置に記憶される機密データを取得して暗号処理手段に与え、第４のセッション鍵により暗号化された機密データをインターフェース手段を介して提供先に対して提供するために出力する。

【００３９】

好ましくは、手順特定情報は、出力手順を特定する第４のセッション鍵であり、制御手段は、第２の復号処理手段によって第３のセッション鍵により暗号化された第４のセッション鍵が復号されるごとに手順特定情報を更新する。

【００４０】

好ましくは、機密データは、その機密データに固有の識別コードを含み、制御手段は、アドレスによって特定される第１の記憶手段上の記憶位置に記憶されている機密データに含まれる識別コードとログ情報に含まれる識別コードとが一致しないとき、機密データの出力を行なうことなく、出力手順を中止する。

【００４１】

好ましくは、データ記憶装置は、インターフェース手段を介して機密データの提供先から受取った、提供先のログ情報に対する署名データが提供先のログ情報

に添付された署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、第１の記憶手段に記憶された機密データをインターフェース手段を介して出力する出力手順が中断した場合、中断した出力手順を再開する再出力手順において、ログ認証手段は、中断した出力手順における機密データの提供先から受取った署名付きログ情報の正当性を検証し、制御手段は、署名付きログ情報が正当でないと判断されたとき、または、署名付きログ情報が正当であると認証され、かつ、署名付きログ情報と当該データ記憶装置の第２の記憶手段に記憶される当該データ記憶装置のログ情報とに基づいて出力手順が中断していないと判断したとき、再出力手順を中止する。

【００４２】

好ましくは、データ記憶装置は、インターフェース手段を介して機密データの提供先から受取った、第４のセッション鍵によって提供先のログ情報に署名されたもう１つの署名付きログ情報の正当性を検証して認証するログ認証手段をさらに備え、第１の記憶手段に記憶された機密データをインターフェース手段を介して出力する出力手順が中断した場合、中断した出力手順を再開する再出力手順において、ログ認証手段は、中断した出力手順における機密データの提供先から受取ったもう１つの署名付きログ情報の正当性を検証し、制御手段は、もう１つの署名付きログ情報が正当でないと判断されたとき、または、もう１つの署名付きログ情報が正当であると認証され、かつ、もう１つの署名付きログ情報と当該データ記憶装置の第２の記憶手段に記憶される当該データ記憶装置のログ情報とに基づいて出力手順が中断していないと判断したとき、再出力手順を中止する。

【００４３】

好ましくは、機密データは、暗号化されたコンテンツデータを復号して利用するための復号鍵であって、暗号化されたコンテンツデータを記憶するための第３の記憶手段をさらに備える。

【００４４】

好ましくは、第３の記憶手段は、ハードディスクである。

【００４５】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

【００４６】

［実施の形態１］

図１は、本発明によるデータ記憶装置が、暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

【００４７】

なお、以下では、デジタル放送網により配信された映像データを端末装置１０により受信して端末装置１０に装着されたデータ記憶装置であるＨＤ（ハードディスク）２０に記憶し、また、暗号化された映像データを復号するためのライセンスを双方向のネットワーク３０に接続される端末装置１０によりネットワーク３０を介してライセンス提供装置４０から受信してＨＤ２０に格納し、暗号化された映像データを端末装置１０に内蔵された専用の再生回路（図示せず）にて再生するデータ配信システムの構成を例にとって説明する。一方、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、音楽データ、教材データ、朗読データ、書籍データ、ゲームなどのプログラムが扱われる場合においても適用することが可能なものである。また、データ記憶装置についても同様で、ハードディスクに限定されることなく、他のデータ記憶装置、たとえばメモリカードなどにおいても適用することが可能である。

【００４８】

図１を参照して、端末装置１０は、デジタル放送網により配信される、暗号化された映像データ（以下、コンテンツデータとも呼ぶ）をアンテナ１１を介して受信し、ＨＤ２０に記憶する。暗号化されたコンテンツデータを復号するためのコンテンツ鍵を含むライセンスを管理し配信するライセンス提供装置４０は、ライセンスの配信を求めてアクセスしてきた端末装置１０に装着されたＨＤ２０が正当な認証データを持つか否か、すなわち、ライセンス管理機能を備えた正規のデータ記憶装置であるか否かの認証処理を行ない、ＨＤ２０が正当なデータ記憶

装置であった場合のみ、端末装置１０に対してＨＤ２０においてのみ復号可能な所定の暗号方式によって暗号化したライセンスを送信する。そして、端末装置１０は、ネットワーク３０に接続されたモデムを介して暗号化されたライセンスを受信すると、その暗号化されたライセンスを装着されたＨＤ２０へ送信する。

【００４９】

図１においては、たとえば、ＨＤ２０は、端末装置１０に着脱可能な構成となっている。端末装置１０に装着されたＨＤ２０は、端末装置１０により受信された暗号化されたライセンスを受取り、著作権を保護するためにライセンス対してなされている暗号化を復号したうえでＨＤ２０内に記憶する。そして、ライセンスに対応した暗号化コンテンツデータを再生する場合、ライセンスに含まれるコンテンツ鍵と暗号化コンテンツデータとを端末装置１０に与える。

【００５０】

そして、端末装置１０のユーザは、端末装置１０においてコンテンツ鍵を用いて復号されるコンテンツデータを再生することが可能となる。

【００５１】

このような構成とすることで、端末装置１０のユーザは、ライセンス管理機能を備え、正規な認証データを有するＨＤ２０を利用しないと、暗号化されたコンテンツデータを受信して記憶したところでライセンスの提供を受けることができず、コンテンツデータを再生することができない。

【００５２】

なお、上述したデータ配信システムにおいては、暗号化コンテンツデータの提供元は、デジタル放送業者の放送サーバであるが、コンテンツのライセンスを管理するライセンス提供装置４０であってもよいし、インターネットなどの通信網を介して接続されるライセンス提供装置４０とは別の配信サーバであってもよく、また、他のユーザからの複製であってもよい。すなわち、暗号化コンテンツデータ自体は、どこから発信されても、また、どこで受信されてもよく、要は暗号化コンテンツデータを復号可能なライセンスを厳重に管理しておきさえすれば、コンテンツデータの著作権を保護することができる。

【００５３】

したがって、本発明の実施の形態においては、ＨＤ２０、端末装置１０およびライセンス提供装置４０のそれぞれの間で行なわれるライセンスの送受信処理において、暗号化コンテンツデータを再生するために必要なライセンスの提供元が、提供先に対する認証およびチェック機能を行ない、非認証の装置に対するライセンスの出力を防止する。さらに、ライセンスの送受信処理中に異常が発生したときに、ライセンスが重複して存在することがないように、再処理の必要なライセンスを特定することでコンテンツデータの著作権保護を実現しつつ、不慮の送受信処理の異常終了から回復可能なシステムの構成について説明する。

【００５４】

図２は、図１に示したデータ配信システムにおいて送受信されるデータ、情報等の特性を説明する図である。

【００５５】

データＤｃは、コンテンツデータであって、ここでは映像データである。データＤｃは、コンテンツ鍵Ｋｃで復号可能な暗号化が施される。コンテンツ鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）が、この形式でデジタル放送網により端末装置１０のユーザに配布される。

【００５６】

なお、以下においては、Ｅ（Ｘ，Ｙ）という表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。また、データＤｃに付随して、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄｉが配布される。

【００５７】

また、ライセンスの配信を特定するとともに、各々のライセンスを特定する管理コードであるライセンスＩＤ（ＬＩＤ）が端末装置１０を介してライセンス提供装置４０とＨＤ２０との間でやり取りされる。さらに、ライセンスとしては、データＤｃおよびコンテンツ鍵Ｋｃを識別するためのコードであるデータＩＤ（ＤＩＤ）や、利用者側からの指定によって決定されるライセンス数や機能限定など、データ記憶装置におけるライセンスや再生の取扱いに対する制限に関する制御情報ＡＣが存在する。

【００５８】

コンテンツ鍵Ｋｃと、制御情報ＡＣと、ＤＩＤと、ＬＩＤとを併せて、以後、ライセンスＬＩＣと総称することとする。ＤＩＤは、データＤｃとコンテンツ鍵Ｋｃとの対に対して割り当てられた識別情報、すなわち、暗号化データＥ（Ｋｃ，Ｄｃ）を識別するための識別情報となる。ＤＩＤは、ライセンスＬＩＣの他に、暗号化データＥ（Ｋｃ，Ｄｃ）とともに常に扱われる付加情報Ｄｉにも含まれ、参照できるようになっている。

【００５９】

図３は、図１に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

【００６０】

ＨＤ２０などのデータ記憶装置および端末装置１０などに備えられる再生回路には、固有のクラス公開鍵ＫＰｃｍｙおよびＫＰｃｐｙがそれぞれ設けられ、クラス公開鍵ＫＰｃｍｙおよびＫＰｃｐｙは、データ記憶装置に固有のクラス秘密鍵Ｋｃｍｙおよび再生回路に固有のクラス秘密鍵Ｋｃｐｙによってそれぞれ復号可能である。これらクラス公開鍵およびクラス秘密鍵は、再生回路あるいはデータ記憶装置の種類ごとに異なる値を持ち、これらクラス公開鍵およびクラス秘密鍵を共有する単位をクラスと称する。記号「ｙ」は、そのクラスを識別するための識別子を表わす。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

【００６１】

また、データ記憶装置のクラス証明書としてＣｍｙが設けられ、再生回路のクラス証明書としてＣｐｙが設けられる。これらのクラス証明書は、データ記憶装置および再生回路のクラスごとに異なる情報を有する。

【００６２】

データ記憶装置のクラス証明書Ｃｍｙは、ＫＰｃｍｙ／／Ｉｃｍｙ／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍｙ／／Ｉｃｍｙ））の形式で出荷時にデータ記憶装置に記憶され、再生回路のクラス証明書Ｃｐｙは、ＫＰｃｐｙ／／Ｉｃｐｙ／／Ｅ（Ｋａ，Ｈ（ＫＰｃｐｙ／／Ｉｃｐｙ））の形式で出荷時に再生回路に記憶される。ここ

で、Ｘ／／Ｙは、ＸとＹとの連結を表わし、Ｈ（Ｘ）は、ハッシュ関数により演算されたデータＸのハッシュ値を表わす。マスタ鍵Ｋａは、これらのクラス証明書を作成するために使用される秘密暗号鍵であり、このデータ配信システム全体で共通の秘密暗号鍵であって、認証局によって安全に管理運用される。また、クラス情報Ｉｃｍｙ，Ｉｃｐｙは、クラスごとの機器に関する情報およびクラス公開鍵を含む情報データである。

【００６３】

また、Ｅ（Ｋａ，Ｈ（ＫＰｃｍｙ／／Ｉｃｍｙ））およびＥ（Ｋａ，Ｈ（ＫＰｃｐｙ／／Ｉｃｐｙ））は、それぞれＫＰｃｍｙ／／ＩｃｍｙおよびＫＰｃｐｙ／／Ｉｃｐｙに対する電子署名を行なった署名データである。

【００６４】

なお、認証局は、署名データを作成する公的機関であり、署名データＥ（Ｋａ，Ｈ（ＫＰｃｍｙ／／Ｉｃｍｙ））およびＥ（Ｋａ，Ｈ（ＫＰｃｐｙ／／Ｉｃｐｙ））は、認証局によって生成される。

【００６５】

さらに、データ記憶装置に対して安全かつ確実にライセンスＬＩＣを送信するための鍵として、データ記憶装置という媒体ごとに設定される個別公開鍵ＫＰｏｍｚと、個別公開鍵ＫＰｏｍｚで暗号化されたデータを復号することが可能な個別秘密鍵Ｋｏｍｚとが存在する。ここで、記号「ｚ」は、データ記憶装置を個別に識別するための識別子である。

【００６６】

データ配信システムにおいてデータの送受信が行なわれるごとに、ライセンス提供装置４０、データ記憶装置（ＨＤ２０）、および端末装置１０の再生回路において生成されるセッション鍵Ｋｓ１ｘ，Ｋｓ２ｘが用いられる。

【００６７】

ここで、セッション鍵Ｋｓ１ｘ，Ｋｓ２ｘは、ライセンス提供装置４０、データ記憶装置（ＨＤ２０）、もしくは端末装置１０の再生回路間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵である。「セッション」には、ライセンス提供装置４０からデータ記憶装置（ＨＤ２０）

へライセンスを配信する「配信セッション」、データ記憶装置間でのライセンスの複製や移動を行なう「複製・移動セッション」、およびデータ記憶装置（ＨＤ２０）から端末装置１０の再生回路へライセンスを出力する「再生許諾セッション」がある。

【００６８】

これらのセッション鍵Ｋｓ１ｘ，Ｋｓ２ｘは、各セッションごとに固有の値を有することにより、ライセンス提供装置４０、データ記憶装置（ＨＤ２０）、および端末装置１０の再生回路によって管理される。具体的には、セッション鍵Ｋｓ１ｘは、ライセンスを送受信する際に、ライセンスの送信側によってセッションごとに発生され、セッション鍵Ｋｓ２ｘは、ライセンスの受信側によってセッションごとに発生される。なお、記号「ｘ」は、セッションにおける一連の処理を識別するための識別子である。そして、各セッションにおいてこれらのセッション鍵を各機器間で相互に授受し、他の機器で生成されたセッション鍵を受けて、そのセッション鍵による暗号化を実行したうえで、ライセンスＬＩＣ、またはコンテンツ鍵を含むライセンスＬＩＣの一部の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

【００６９】

図４は、図１に示したライセンス提供装置４０の構成を示す概略ブロック図である。

【００７０】

ライセンス提供装置４０は、管理対象のライセンスを保持するデータベースであるコンテンツＤＢ４０２と、ライセンスを配信する配信セッションにおける一切の通信記録を記憶保持するデータベースであるログＤＢ４０４と、コンテンツＤＢ４０２およびログＤＢ４０４とバスＢＳ１を介してデータをやり取りし、所定の処理を行なうためのデータ処理部４１０と、ネットワーク３０を介して端末装置１０とデータ処理部４１０との間でデータ授受を行なうための通信装置４５０とを備える。

【００７１】

データ処理部４１０は、バスＢＳ１上のデータに応じて、データ処理部４１０

の動作を制御するための配信制御部４１２と、配信制御部４１２により制御されて、配信セッション時にセッション鍵Ｋｓ１ｘを発生するためのセッション鍵発生部４１４と、端末装置１０から送られてくるＨＤ２０のクラス証明書Ｃｍｙに含まれる署名データＥ（Ｋａ，Ｈ（ＫＰｃｍｙ／／Ｉｃｍｙ））を復号するためのＨＤ２０の認証鍵ＫＰａを保持するＫＰａ保持部４１６と、ＨＤ２０から送られてきたクラス証明書Ｃｍｙを通信装置４５０およびバスＢＳ１を介して受け、ＫＰａ保持部４１６から受ける認証鍵ＫＰａによって復号処理を行ない、クラス証明書Ｃｍｙに含まれる署名データＥ（Ｋａ，Ｈ（ＫＰｃｍｙ／／Ｉｃｍｙ））の復号処理と、クラス証明書Ｃｍｙに含まれるＫＰｃｍｙ／／Ｉｃｍｙのハッシュ値の計算を行ない、両者の結果を比較チェックしてクラス証明書Ｃｍｙの検証を行なう認証部４１８と、配信セッションごとに、セッション鍵発生部４１４により生成されたセッション鍵Ｋｓ１ｘを認証部４１８によってクラス証明書Ｃｍｙから抽出したクラス公開鍵ＫＰｃｍｙを用いて暗号化し、バスＢＳ１に出力するための暗号処理部４２０と、セッション鍵Ｋｓ１ｘによって暗号化された上で送信されたデータをバスＢＳ１より受け、復号処理を行なう復号処理部４２２とを含む。

【００７２】

データ処理部４１０は、さらに、配信制御部４１２から与えられるライセンスＬＩＣを、復号処理部４２２によって得られたデータ記憶装置ごとに固有な個別公開鍵ＫＰｏｍｚによって暗号化するための暗号処理部４２４と、暗号処理部４２４の出力を、復号処理部４２２から与えられるセッション鍵Ｋｓ２ｘによってさらに暗号化してバスＢＳ１に出力するための暗号処理部４２６とを含む。

【００７３】

なお、個別公開鍵ＫＰｏｍｚおよびセッション鍵Ｋｓ２ｘは、セッション鍵Ｋｓ１ｘによって暗号化されたうえで端末装置１０から提供される。復号処理部４２２は、これを復号して個別公開鍵ＫＰｏｍｚを得る。

【００７４】

ライセンス提供装置４０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００７５】

図５は、図１に示した端末装置１０の構成を説明するための概略ブロック図である。

【００７６】

端末装置１０は、デジタル放送網によって伝送される信号を受信するアンテナ１０２と、アンテナ１０２からの信号を受けてベースバンド信号に変換、あるいはアンテナ１０２から送信するデータを変調してアンテナ１０２に与える受信部１０４と、端末装置１０をネットワーク３０に接続するモデム１０６と、端末装置１０の各部のデータ授受を行なうバスＢＳ２と、バスＢＳ２を介して端末装置１０の動作を制御するコントローラ１０８と、ＨＤ２０とバスＢＳ２との間のデータの授受を制御するＨＤインタフェース部１１０とを含む。

【００７７】

端末装置１０は、さらに、上述したクラス証明書Ｃｐｙを保持する認証データ保持部１５０２を含む。ここで、端末装置１０のクラスｙは、ｙ＝３であるとする。

【００７８】

端末装置１０は、さらに、クラス固有の復号鍵であるクラス秘密鍵Ｋｃｐ３を保持するＫｃｐ保持部１５０４と、バスＢＳ２から受けたデータをクラス秘密鍵Ｋｃｐ３によって復号し、ＨＤ２０によって発生されたセッション鍵Ｋｓ１ｘを得る復号処理部１５０６とを含む。

【００７９】

端末装置１０は、さらに、ＨＤ２０に記憶されたコンテンツデータの再生を行なう再生許諾セッションにおいて、ＨＤ２０との間でやり取りされるデータを暗号化するためのセッション鍵Ｋｓ２ｘを乱数等により発生するセッション鍵発生部１５０８と、ＨＤ２０からコンテンツ鍵Ｋｃを受取る際に、セッション鍵発生部１５０８により発生されたセッション鍵Ｋｓ２ｘを復号処理部１５０６によって得られたセッション鍵Ｋｓ１ｘによって暗号化し、バスＢＳ２に出力する暗号処理部１５１０と、バスＢＳ２上のデータをセッション鍵Ｋｓ２ｘによって復号して、コンテンツ鍵Ｋｃを出力する復号処理部１５１２と、バスＢＳ２より暗号

化コンテンツデータＥ（Ｋｃ，Ｄｃ）を受けて、復号処理部１５１２からのコンテンツ鍵Ｋｃによって暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を復号してデータＤｃを再生部１５１６へ出力する復号処理部１５１４と、復号処理部１５１４からの出力を受けてコンテンツを再生するための再生部１５１６と、再生部１５１６の出力をデジタル信号からアナログ信号に変換するＤＡ変換部１５１８と、ＤＡ変換部１５１８の出力をテレビモニターなどの外部出力装置（図示省略）へ出力するための端子１５２０とを含む。

【００８０】

なお、図５においては、点線で囲んだ領域は暗号化コンテンツデータを復号して映像データを再生する専用回路である再生回路１５０を構成する。再生回路１５０は、セキュリティを向上させるために１チップ構成の半導体デバイスであることが好ましい。さらには、再生回路１５０は、外部からの解析が困難な耐タンパモジュールとして構成されることが好ましい。

【００８１】

端末装置１０の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

【００８２】

図６は、図１に示すＨＤ２０の構成を説明するための概略ブロック図である。

すでに説明したように、ハードディスクのクラス公開鍵およびクラス秘密鍵として、ＫＰｃｍｙおよびＫｃｍｙが設けられ、ハードディスクのクラス証明書Ｃｍｙが設けられるが、ＨＤ２０においては、自然数ｙ＝１で表わされるものとする。また、ＨＤ２０を識別する自然数ｚはｚ＝２で表されるものとする。

【００８３】

したがって、ＨＤ２０は、クラス証明書Ｃｍ１として認証データＫＰｃｍ１／／Ｉｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を保持する認証データ保持部２０２と、クラス秘密鍵Ｋｃｍ１を保持するＫｃｍ保持部２０４と、個別秘密鍵Ｋｏｍ２を保持するＫｏｍ保持部２０６と、個別秘密鍵Ｋｏｍ２によって復号可能な個別公開鍵ＫＰｏｍ２を保持するＫＰｏｍ保持部２０８とを含む。

【００８４】

このように、ハードディスクドライブというデータ記憶装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたコンテンツ鍵の管理をハードディスクドライブ単位で実行することが可能になる。

【００８５】

ＨＤ２０は、さらに、端末装置１０のＨＤインターフェース部１１０と端子２１０を介して信号を授受するＡＴＡ（ＡＴ－Ａｔｔａｃｈｍｅｎｔ）インタフェース部２１２と、ＨＤ２０におけるデータ伝送路であるバスＢＳ３と、ＡＴＡインターフェース部２１２からコントローラ２１４を介してバスＢＳ３に出力されたデータを、Ｋｏｍ保持部２０６により与えられた個別秘密鍵Ｋｏｍ２により復号し、ライセンス提供装置４０から配信されたライセンスＬＩＣをセキュアデータ記憶部２５０へ出力する復号処理部２１６と、ＫＰａ保持部２１８から認証鍵ＫＰａを受け、バスＢＳ３に出力されたデータの認証鍵ＫＰａによる復号処理を実行して復号結果をコントローラ２１４へ出力し、かつ、得られたクラス公開鍵ＫＰｃｍ１を暗号処理部２２２へ出力する認証部２２０と、切換スイッチ２６０によって選択的に与えられるセッション鍵Ｋｓ１ｘまたは Ｋｓ２ｘによって、切換スイッチ２６２によって選択的に与えられるデータを暗号化してバスＢＳ３に出力する暗号処理部２２４とを含む。

【００８６】

ＨＤ２０は、さらに、配信、複製・移動、および再生許諾の各セッションにおいて、セッション鍵Ｋｓ１ｘ，Ｋｓ２ｘを発生するセッション鍵発生部２２６と、セッション鍵発生部２２６の出力したセッション鍵Ｋｓ１ｘを認証部２２０によって得られる端末装置１０の再生回路１５０のクラス公開鍵ＫＰｃｐｙあるいは他のデータ記憶装置（ＨＤ２１とする）のクラス公開鍵ＫＰｃｍｙによって暗号化してバスＢＳ３に送出する暗号処理部２２２と、バスＢＳ３よりセッション鍵Ｋｓ２ｘによって暗号化されたデータを受けてセッション鍵発生部２２６より得たセッション鍵Ｋｓ１ｘまたは Ｋｓ２ｘによって復号する復号処理部２２８とを含む。

【００８７】

ＨＤ２０は、さらに、バスＢＳ３上のデータをクラス公開鍵ＫＰｃｍ１と対をなすクラス秘密鍵Ｋｃｍ１によって復号するための復号処理部２３０と、ライセンスＬＩＣをＨＤ２０からＨＤ２１へ移動または複製するために出力する際に、提供先のＨＤ２１から受信した個別公開鍵ＫＰｏｍｚ（ｚ≠２）によりライセンスＬＩＣを暗号化する暗号処理部２３２とを含む。

【００８８】

ＨＤ２０は、さらに、暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を再生するためのライセンスＬＩＣと、ＨＤ２０が処理しているセッションの処理記録であるログとをバスＢＳ３より受けて記憶するセキュアデータ記憶部２５０を含む。そして、ライセンスＬＩＣは、セキュアデータ記憶部２５０内のセキュアデータメモリ２５０Ａに格納され、ログは、セキュアデータ記憶部２５０内のログメモリ２５０Ｂに格納される。セキュアデータ記憶部２５０は、たとえば半導体メモリによって構成される。

【００８９】

図７は、セキュアデータ記憶部２５０におけるメモリ構成を示した図である。

図７を参照して、セキュアデータメモリ２５０Ａは、ＨＤ２０が複数のコンテンツデータを記憶可能であることに対応して、ライセンスＬＩＣ（コンテンツ鍵Ｋｃ、制御情報ＡＣ、ライセンスＩＤ（ＬＩＤ）、データＩＤ（ＤＩＤ））を複数格納することができる構成になっている。

【００９０】

そして、ＨＤ２０においては、セキュアデータメモリ２５０Ａに格納されたライセンスＬＩＣは、セキュアデータ記憶部２５０における格納アドレス（以下、ＬＢＡ；Ｌｏｇｉｃａｌ　Ｂｌｏｃｋ　Ａｄｄｒｅｓｓと称する。）により管理される。そして、各セッションにおいて記憶あるいは出力されるライセンスＬＩＣは、全てＬＢＡにより特定される。

【００９１】

また、セキュアデータ記憶部２５０には、有効フラグメモリ２５０Ｃが設けられる。有効フラグメモリ２５０Ｃは、セキュアデータメモリ２５０Ａ上の記憶位置を特定するＬＢＡそれぞれに対応して設けられ、対応するＬＢＡによって特定

される位置に記憶されるライセンスの有効性を示すフラグを記憶する。

【００９２】

有効フラグメモリ２５０Ｃのフラグが「有効」であるとき、フラグに対応するＬＢＡによって特定されるセキュアデータメモリ２５０Ａ上の記憶位置に記憶されているライセンスＬＩＣは利用可能であり、ユーザはそのライセンスＬＩＣに対応したコンテンツデータを再生したり、そのライセンスＬＩＣの移動・複製を行なうことができる。

【００９３】

一方、有効フラグメモリ２５０Ｃのフラグが「無効」であるとき、そのフラグに対応するＬＢＡによって特定されるセキュアデータメモリ２５０Ａ上の記憶位置に記憶されているライセンスＬＩＣは利用不可であり、ＨＤ２０のコントローラ２１４によって、そのＬＢＡからのライセンスＬＩＣは拒否される。すなわち、消去されたのと同じ状態である。したがって、ユーザはそのライセンスＬＩＣに対応したコンテンツデータを再生することはできない。この有効フラグメモリ２５０Ｃのフラグは、ライセンスの新たな記憶によって「有効」とされ、ライセンスの移動によって「無効」とされる。

【００９４】

ログメモリ２５０Ｂには、セッションの対象となるライセンスＬＩＣを特定するライセンスＩＤ（ＬＩＤ）を格納するライセンスＩＤ領域２５０１、セッションにおいてライセンスＬＩＣの受信側のデータ記憶装置によって生成されたセッション鍵Ｋｓ２ｘを格納するＫｓ２ｘ領域２５０２、動作中のセッションにおける処理の状態を示すステータスＳＴ１を格納するＳＴ１領域２５０３およびライセンスＩＤ領域２５０１に格納されるライセンスＩＤに対応したライセンスの記憶状態を示すステータスＳＴ２を格納するＳＴ２領域２５０４、ライセンスを移動・複製によって出力する場合、送信側のデータ記憶装置において受信側のデータ記憶装置のクラス公開鍵ＫＰｃｍｘを格納するＫＰｃｍｘ領域２５０５、並びに当該セッションにおいてライセンスＬＩＣを出力あるいは記憶するために指示されたＬＢＡを格納するＬＢＡ領域２５０６が設けられ、一連のセッションの処理が進行するにつれて、上記各領域のデータが更新あるいは参照されていく。ス

テータスＳＴ１は、「受信待」、「受信済」、「送信待」および「送信済」の４状態のいずれかであり、ステータスＳＴ２は、「データ有」、「データ無」および「移動済」の３状態のいずれかである。

【００９５】

そして、セッション中に予期しない異常が発生し、セッションが中断した場合、そのセッションにおいて送受信されていたライセンスＬＩＣに対して、ログメモリ２５０Ｂ内のＬＩＤ領域２５０１に格納されているライセンスＩＤと、ＬＢＡ領域２５０６に格納されたＬＢＡとによって当該ライセンスＬＩＣの記憶状態が確認され、その確認結果に応じてステータスＳＴ２が更新される。また、中断したセッションにおけるライセンスの送信側では、ライセンスの受信側のログメモリ２５０Ｂ内に格納されているライセンスＬＩＣ、セッション鍵Ｋｓ２ｘ、ステータスＳＴ１およびステータスＳＴ２を受取って、自身が記録するログの内容と受取ったライセンスＬＩＣ、セッション鍵Ｋｓ２ｘ、ステータスＳＴ１およびステータスＳＴ２とを確認することにより、再度のライセンスの送受信を行なってもよいか否かの判断がされる。

【００９６】

なお、セッション鍵Ｋｓ２ｘは、各セッションを特定するために記憶され、セッション鍵Ｋｓ２ｘを共有していることは、ライセンスの送受信先およびその処理を共有していたことを示している。

【００９７】

このような構成とすることにより、特に、相当数のライセンスがセキュアデータメモリ２５０Ａに格納されているときに、あるセッションにおける処理の中断が発生したときなどセキュアデータメモリ２５０Ａにおけるライセンスを特定する必要があるときに（あるいはライセンスの有無を特定）、容易にライセンスの記憶状態を確認し、ステータスＳＴ２を更新できる。

【００９８】

なお、以下、再送信の確認時においてライセンスの受信側となった場合に、ライセンスの送信側に対して出力するログメモリ２５０Ｂに格納されたライセンスＩＤ（ＬＩＤ）、セッション鍵Ｋｓ２ｘおよびステータスＳＴ１，ＳＴ２は、出

力ログと総称する。また、ＨＤ２０においてのみ参照されるログメモリ２５０Ｂに格納された受信側のクラス公開鍵ＫＰｃｍｘおよびＬＢＡは、内部ログと総称する。

【００９９】

また、ステータスＳＴ２には、出力ログが出力される際に、ログメモリ２５０Ｂに格納されているライセンスＩＤ（ＬＩＤ）とＬＢＡとによってセキュアデータメモリ２５０Ａにおける対象のライセンスの記憶状態が格納され、これによって出力ログが成立する。

【０１００】

詳細については、後ほど各セッション毎のフローチャートを使用して説明する。

【０１０１】

ここで、再び図６を参照して、ＨＤ２０のデータ記録部に関して説明する。ＨＤ２０は、さらに、暗号化コンテンツデータを記憶するノーマルデータ記憶部２７０を含む。ノーマルデータ記憶部２７０は、データが記憶される円盤状の磁気記録媒体２７０１と、磁気記録媒体２７０１を回転させるモータ２７０２と、モータ２７０２を制御するサーボ制御部２７０３と、磁気記録媒体２７０１上における磁気ヘッドの位置を制御するシーク制御部２７０４と、磁気ヘッドへデータの記録および再生を指示する記録再生処理部２７０５とを含む。ノーマルデータ記憶部２７０の構成は、一般の公知のハードディスクの構成と変わるところはなく、詳細な説明は省略する。

【０１０２】

ＨＤ２０は、さらに、ＡＴＡインターフェース部２１２を介して外部との間でデータ授受、制御情報ＡＣに基づくライセンスの出力に関する判断、およびセキュアデータ記憶部２５０の管理などのＨＤ２０内の動作を制御するためのコントローラ２１４を含む。

【０１０３】

なお、ノーマルデータ記憶部２７０、ＡＴＡインターフェース部２１２および端子２１０を除く他の構成は、耐タンパモジュール領域に構成される。

【０１０４】

以下、図１に示すデータ配信システムにおける各セッションの動作について説明する。

【０１０５】

［配信］

まず、図１に示すデータ配信システムにおいて、ライセンス提供装置４０から端末装置１０に装着されたＨＤ２０へライセンスを配信する動作について説明する。

【０１０６】

図８および図９は、図１に示すデータ配信システムにおいて、端末装置１０のユーザが端末装置１０から暗号化コンテンツデータのライセンス配信のリクエストを行なうことにより、ライセンス提供装置４０から端末装置１０に装着されたＨＤ２０へライセンスの配信が行なわれる際の処理（配信セッション）を説明するための第１および第２のフローチャートである。

【０１０７】

図８における処理開始以前に、端末装置１０のユーザは、端末装置１０をモデム１０６によりネットワーク３０に接続し、端末装置１０をネットワーク３０を介してライセンス提供装置４０に接続していることを前提としている。

【０１０８】

図８を参照して、端末装置１０のユーザから所望のコンテンツデータのライセンスに対する配信リクエストがなされると、端末装置１０のコントローラ１０８は、バスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へクラス証明書の出力要求を出力する（ステップＳ１）。ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインタフェース部２１２を介してクラス証明書の出力要求を受理すると（ステップＳ２）、バスＢＳ３を介して認証データ保持部２０２からクラス証明書Ｃｍ１＝ＫＰｃｍ１／／Ｉｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を読出し、クラス証明書Ｃｍ１をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ３）

。

【０１０９】

端末装置１０のコントローラ１０８は、ＨＤ２０からＨＤインターフェース部１１０およびバスＢＳ２を介してクラス証明書Ｃｍ１を受理すると（ステップＳ４）、受理したクラス証明書Ｃｍ１をモデム１０６およびネットワーク３０を介してライセンス提供装置４０へ送信する（ステップＳ５）。

【０１１０】

ライセンス提供装置４０では、端末装置１０からクラス証明書Ｃｍ１を受信すると（ステップＳ６）、受信したＣｍ１が正当なクラス証明書であるか否かを検証する（ステップＳ７）。検証処理は次のように行なわれる。

【０１１１】

ライセンス提供装置４０は、クラス証明書Ｃｍ１＝ＫＰｃｍ１／／Ｉｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を受理すると、ＨＤ２０から出力されたクラス証明書Ｃｍ１に含まれる署名データＥ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を認証部４１８において認証鍵ＫＰａで復号する。そして、さらに、認証部４１８は、クラス証明書Ｃｍ１に含まれるＫＰｃｍ１／／Ｉｃｍ１のハッシュ値を演算し、認証鍵ＫＰａで復号したＨ（ＫＰｃｍ１／／Ｉｃｍ１）の値と比較する。配信制御部４１２は、認証部４１８における復号処理結果から、上記の復号ができ、かつ、ハッシュ値の値が一致したと判断すると、ＨＤ２０から受理したクラス証明書Ｃｍ１は、正当な証明書であると判断する。

【０１１２】

ステップＳ７において、クラス証明書Ｃｍ１が正当な証明書であると判断された場合、配信制御部４１８は、クラス証明書Ｃｍ１を承認し、クラス公開鍵ＫＰｃｍ１を受理する（ステップＳ８）。そして、次の処理（ステップＳ９）へ移行する。正当なクラス証明書でない場合には、配信制御部４１２はクラス証明書Ｃｍ１を非承認とし、クラス証明書Ｃｍ１を受理しないでエラー通知を端末装置１０へ出力し（図９のステップＳ４４）、端末装置１０においてエラー通知が受理されると（図９のステップＳ４５）、配信セッションが終了する。

【０１１３】

認証の結果、ライセンス提供装置４０において、正当なクラス証明書を持つハ

ードディスクを装着した端末装置からのアクセスであることが確認され、ステップＳ８においてクラス公開鍵ＫＰｃｍ１が受理されると、配信制御部４１２は、ライセンスＩＤ（ＬＩＤ）を生成し（ステップＳ９）、さらに制御情報ＡＣを生成する（ステップＳ１０）。そして、セッション鍵発生部４１４は、配信のためのセッション鍵Ｋｓ１ａを生成する（ステップＳ１１）。セッション鍵Ｋｓ１ａは、認証部４１８によって得られたＨＤ２０に対応するクラス公開鍵ＫＰｃｍ１によって、暗号処理部４２０によって暗号化され、暗号データＥ（ＫＰｃｍ１，Ｋｓ１ａ）が生成される（ステップＳ１２）。

【０１１４】

そして、配信制御部４１２は、ライセンスＩＤ（ＬＩＤ）および暗号化されたセッション鍵Ｋｓ１ａを１つのデータ列ＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）として、バスＢＳ１および通信装置４５０を介して外部に出力する（ステップＳ１３）。

【０１１５】

端末装置１０は、ネットワーク３０を介してＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受信すると（ステップＳ１４）、受信したＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）をＨＤ２０へ出力する（ステップＳ１５）。そして、ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインタフェース部２１２を介してＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受理する（ステップＳ１６）。コントローラ２１４は、バスＢＳ３を介して受理したＥ（ＫＰｃｍ１，Ｋｓ１ａ）を復号処理部２３０へ与え、復号処理部２３０は、Ｋｃｍ保持部２０４に保持されるＨＤ２０に固有なクラス秘密鍵Ｋｃｍ１によって復号処理することにより、セッション鍵Ｋｓ１ａを復号し、セッション鍵Ｋｓ１ａを受理する（ステップＳ１７）。

【０１１６】

ＨＤ２０のコントローラ２１４は、ライセンス提供装置４０で生成されたセッション鍵Ｋｓ１ａの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して、ＨＤ

２０においてセッション鍵Ｋｓ１ａが受理された旨の通知を受理すると、ＨＤ２０において配信動作時に生成されるセッション鍵の生成の要求通知をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する（ステップＳ１８）。ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡコントローラ２１２を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部２２６に対してＨＤ２０において配信動作時に生成されるセッション鍵Ｋｓ２ａの生成を指示する。そして、セッション鍵発生部２２６は、セッション鍵Ｋｓ２ａを生成する（ステップＳ１９）。

【０１１７】

セッション鍵発生部２２６は、セッション鍵Ｋｓ２ａを生成すると、バスＢＳ３を介してコントローラ２１４へ出力し、セッション鍵Ｋｓ２ａを受けたコントローラ２１４は、ステップＳ１６において受理したライセンスＩＤ（ＬＩＤ）とセッション鍵Ｋｓ２ａとをセキュアデータ記憶部２５０内のログメモリ２５０Ｂへ格納するとともに、ステータスＳＴ１を「受信待」にする（ステップＳ２０）。

【０１１８】

続いて、暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ａによって、切換スイッチ２６２の接点ＰｄとＰｆとを順に切換えることによって与えられるセッション鍵Ｋｓ２ａと個別公開鍵ＫＰｏｍ２とからなる１つのデータ列を暗号化し、Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）生成する（ステップＳ２１）。そして、暗号処理部２２４は、Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をバスＢＳ３に出力する。バスＢＳ３に出力された暗号化データＥ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）は、コントローラ２１４により受理され、コントローラ２１４は、受理した暗号化データとライセンスＩＤ（ＬＩＤ）とを１つのデータ列としたデータＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ２）をＡＴＡインタフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ２２）。

【０１１９】

そして、端末装置１０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰ

ｏｍ2）をＨＤ２０から受理すると（ステップＳ２３）、受理したデータをネットワーク３０を介してライセンス提供装置４０に出力する（ステップＳ２４）。

【０１２０】

ライセンス提供装置４０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ2）を受信すると（ステップＳ２５）、復号処理部４２２においてセッション鍵Ｋｓ１ａによる復号処理を実行し、ＨＤ２０で生成されたセッション鍵Ｋｓ２ａ、およびＨＤ２０の個別公開鍵ＫＰｏｍ２を受理する（ステップＳ２６）。

【０１２１】

配信制御部４１２は、ライセンスＩＤ（ＬＩＤ）に対応するデータＩＤ（ＤＩＤ）およびコンテンツ鍵Ｋｃをコンテンツ ＤＢ４０２から取得し（ステップＳ２７）、ライセンスＩＤ（ＬＩＤ）および制御情報ＡＣと併せた１つのデータ列としてのライセンスＬＩＣ＝Ｋｃ／／ＡＣ／／ＤＩＤ／／ＬＩＤを生成する。

【０１２２】

配信制御部４１２は、生成したライセンスＬＩＣを暗号処理部４２４に与える。暗号処理部４２４は、復号処理部４２２によって得られたＨＤ２０の個別公開鍵ＫＰｏｍ２によってライセンスＬＩＣを暗号化して暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を生成する（ステップＳ２８）。そして、暗号処理部４２６は、暗号処理部４２４から受ける暗号化データＥ（ＫＰｏｍ２，ＬＩＣ）を、復号処理部４２２から受けるセッション鍵Ｋｓ２ａによって暗号化し、暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を生成する（ステップＳ２９）。

【０１２３】

図９を参照して、配信制御部４１２は、バスＢＳ１および通信装置４５０を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を外部へ出力する（ステップＳ３０）。端末装置１０は、ネットワーク３０を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を受理すると（ステップＳ３１）、受理した暗号化データをＨＤ２０へ出力する（ステップＳ３２）。

【０１２４】

ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース

部２１２を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を受理すると（ステップＳ３３）、バスＢＳ３へ出力する。復号処理部２２８は、セッション鍵発生部２２６から与えられたセッション鍵Ｋｓ２ａを用いてバスＢＳ３に出力されたデータＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ２，ＬＩＣ））を復号し、ＨＤ２０において、ライセンスＬＩＣが個別公開鍵ＫＰｏｍ２により暗号化された暗号化ライセンスＥ（ＫＰｏｍ２，ＬＩＣ）が受理される（ステップＳ３４）。そして、復号処理部２２８は、暗号化ライセンスＥ（ＫＰｏｍ２，ＬＩＣ）をバスＢＳ３へ出力する。

【０１２５】

コントローラ２１４の指示によって、暗号化ライセンスＥ（ＫＰｏｍ２，ＬＩＣ）は、復号処理部２１６において個別秘密鍵Ｋｏｍ２によって復号され、ライセンスＬＩＣが受理される（ステップＳ３５）。

【０１２６】

ＨＤ２０のコントローラ２１４は、ライセンスＬＩＣの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して、ＨＤ２０においてライセンスＬＩＣが受理された旨の通知を受理すると、ＨＤ２０のセキュアデータ記憶部２５０において、その受信したライセンスＬＩＣを格納するＬＢＡをバスＢＳ２およびＨＤインターフェース１１０を介してＨＤ２０へ出力する（ステップＳ３６）。ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介してライセンスＬＩＣの格納先ＬＢＡを受理すると（ステップＳ３７）、その受理したＬＢＡをログメモリ２５０Ｂに記憶する（ステップＳ３８）。

【０１２７】

そして、コントローラ２１４は、受理したライセンスＬＩＣに含まれるライセンスＩＤ（ＬＩＤ）と、ステップＳ１６において受理したライセンスＬＩＤ（ＬＩＤ）とを比較し、一致しているか否かをチェックする（ステップＳ３９）。コントローラ２１４は、ＬＩＤが一致しており、受理したライセンスＬＩＣが正しいものであると判断すると、端末装置１０から受理したセキュアデータ記憶部２

５０内のＬＢＡに、受理したライセンスＬＩＣを記憶する（ステップＳ４０）。

【０１２８】

コントローラ２１４は、指定されたＬＢＡにライセンスＬＩＣを記憶すると、有効フラグメモリ２５０Ｃのそのに対応するフラグを「有効」にする（ステップＳ４１）。そして、コントローラ２１４は、さらに、ログメモリ２５０Ｂのステータスを「受信済」にし（ステップＳ４２）、配信セッションにおける一連の処理が終了したことを端末装置１０に通知する。

【０１２９】

そして、端末装置１０において、ＨＤ２０から処理終了通知が受理されると、データ配信システムにおける配信セッションが正常終了する。

【０１３０】

一方、ステップＳ３９において、コントローラ２１４は、ＬＩＤが一致せず、受理したライセンスＬＩＣが正しくないと判断すると、エラー通知を端末装置１０へ出力し（ステップＳ４３）、端末装置１０は、エラー通知を受理すると（ステップＳ４５）、処理を終了する。

【０１３１】

図８および図９に示された配信処理においては、ライセンス提供装置４０における処理履歴の記録に関する記載がなされていないが、図４に示すように、ライセンス提供装置４０には、十分な記憶容量を持つログＤＢ４０４が備えられており、配信セッションにおける各処理の進行に伴う処理履歴がログＤＢ４０４に記憶される。また、ログＤＢ４０４には、ライセンスの送信に伴なう課金情報なども記憶される。

【０１３２】

図８および図９に示された配信処理における一連の処理において、ステップＳ２５からステップＳ４４の処理中に異常が発生して処理が中断したときは、再書込処理の対象となる。たとえば、中断の理由として、上記処理中に端末装置１０の電源が遮断されたり、ライセンス提供装置４０側の異常、あるいは端末装置１０とライセンス提供装置４０との通信異常など、種々の異常ケースが考えられる。ここで、ＨＤ２０内のログメモリ２５０Ｂに格納されたステータスＳＴ２を除

く出力ログの内容がすべて格納されたステップＳ２２終了後からステップＳ４４までの処理中に処理が中断した場合には、ＨＤ２０は、再書込処理を行なってライセンスの提供を受けることが可能である。ここでは、端末装置１０の判断によって再書込処理を行なうものとしたため、端末装置１０において処理の進行が確認できるステップＳ２２からステップＳ２４を除く、ステップＳ２５からステップＳ４４の処理中に処理が中断した場合を再書込処理の対象とし、他のステップにおける処理の中断においてはライセンス提供装置４０からライセンスの提供がなされなかったものと判断し、図８および図９に示したフローチャートにしたがって、最初から処理を行なうこととした。

【０１３３】

同様に、ライセンス提供装置４０がライセンスを出力するまでのライセンス提供装置４０内のステップＳ２５からステップＳ３０までの処理については、端末装置１０において、これらのいずれのステップを処理中に処理が中断したかを特定できる場合には、再書込処理の対象から除外して、図８および図９に示したフローチャートにしたがって、最初から処理を行なうものとしてもよい。

【０１３４】

図１０から図１２は、図８および図９において示した配信処理におけるステップＳ２５からステップＳ４４の処理中に異常が発生したときに行なわれる再書込処理の第１から第３のフローチャートである。

【０１３５】

図１０を参照して、端末装置１０は、ステップＳ２５からステップＳ４４の処理中に異常が発生したと判断すると、ライセンスＬＩＣの再書込要求をネットワーク３０を介してライセンス提供装置４０へ出力する（ステップＳ１０１）。配信制御部４１２は、通信装置４５０およびバスＢＳ１を介して再書込要求を受理すると（ステップＳ１０２）、セッション鍵発生部４１４にセッション鍵を生成するように指示する。指示を受けたセッション鍵発生部４１４は、再書込処理のためのセッションキー鍵Ｋｓ１ｂを生成する（ステップＳ１０３）。そして、配信制御部４１２は、このセッションにおいてＨＤ２０とやり取りしたログが格納されているログＤＢ４０２からＨＤ２０に対応するクラス公開鍵ＫＰｃｍ１を取

得し（ステップＳ１０４）、暗号処理部４２０に与える。クラス公開鍵ＫＰｃｍ１を受けた暗号処理部４２０は、クラス公開鍵ＫＰｃｍ１をによりセッション鍵Ｋｓ１ｂを暗号化し、Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）が生成される（ステップＳ１０５）。そして、配信制御部４１２は、Ｅ（ＫＰｃｍ１，Ｋｓ１ｂ）をバスＢＳ１および通信装置４５０を介して外部に出力する（ステップＳ１０６）。

【０１３６】

端末装置１０は、ネットワーク３０を介してＥ（ＫＰｃｍ１，Ｋｓ１ｂ）を受理すると（ステップＳ１０７）、受理したＥ（ＫＰｃｍ１，Ｋｓ１ｂ）をＨＤ２０へ出力する（ステップＳ１０８）。そして、ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインタフェース部２１２を介してＥ（ＫＰｃｍ１，Ｋｓ１ｂ）を受理する（ステップＳ１０９）。コントローラ２１４は、受理したＥ（ＫＰｃｍ１，Ｋｓ１ｂ）をバスＢＳ３を介して復号処理部２３０へ与え、復号処理部２３０は、Ｋｃｍ保持部２０４に保持されるＨＤ２０に固有なクラス秘密鍵Ｋｃｍ１によって復号処理することにより、セッション鍵Ｋｓ１ｂを復号し、セッション鍵Ｋｓ１ｂが受理される（ステップＳ１１０）。

【０１３７】

ＨＤ２０のコントローラ２１４は、ライセンス提供装置４０で生成されたセッション鍵Ｋｓ１ｂの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して、ＨＤ２０においてセッション鍵Ｋｓ１ｂが受理された旨の通知を受理すると、セキュアデータ記憶部２５０に記憶されたログメモリ２５０Ｂの出力要求をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する（ステップＳ１１１）。

【０１３８】

ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡコントローラ２１２を介してログメモリ２５０Ｂの出力要求通知を受理すると（ステップＳ１１２）、ログメモリ２５０Ｂに格納されたＬＢＡに記憶されるライセンスＬＩＣのライセンスＩＤ（ＬＩＤ）と、ログメモリ２５０Ｂに格納されたライセンスＩＤ（

ＬＩＤ）とが一致するか否かをチェックする（ステップＳ１１３）。

【０１３９】

コントローラ２１４は、両ライセンスＩＤ（ＬＩＤ）が一致すると判断すると、配信処理としては、ライセンス提供装置４０からのライセンスＬＩＣの受理までは行なわれ、ＨＤ２０においてライセンスＬＩＣは受理していると認識する。そうすると、コントローラ２１４は、ログメモリ２５０Ｂに格納されたＬＢＡにより指示されるアドレスに記憶されるライセンスに対応する有効フラグメモリ２５０Ｃに格納されているフラグをチェックして、そのライセンスの有効性をチェックする（ステップＳ１１４）。

【０１４０】

コントローラ２１４は、ライセンスが有効であると判断すると、ログメモリ２５０Ｂのステータスｓｔ２を「データ有」に変更し、次の処理（ステップＳ１１８）へ移行する。一方、コントローラ２１４は、ステップＳ１１４においてライセンスが無効であると判断すると、ログメモリ２５０Ｂのステータスｓｔ２を「移動済」に変更し、次の処理（ステップＳ１１８）へ移行する。

【０１４１】

ステップ１１３において、コントローラ２１４は、比較したライセンスＩＤ（ＬＩＤ）が一致しないと判断したときは、ログメモリ２５０Ｂのステータスｓｔ２を「データ無」に変更する（ステップＳ１１７）。

【０１４２】

このように、ログメモリ２５０Ｂに格納されたＬＢＡを用いて、そのＬＢＡに記憶されるライセンスＬＩＣのライセンスＩＤ（ＬＩＤ）をＬＢＡに基づいて直接確認できるので、セキュアデータメモリ２５０Ａに相当数のライセンスが格納されているときであっても、それらのライセンスを逐一検索することなしに特定のライセンスＩＤ（ＬＩＤ）の有無などを判断することができる。

【０１４３】

ステータスｓｔ２の変更処理がなされると、コントローラ２１４は、ログメモリ２５０Ｂからライセンスｉｄ（ＬＩＤ）、ステータスｓｔ１，ｓｔ２およびセッション鍵Ｋｓ２ｃを取得する（ステップＳ１１８）。ここで、ログメモリ２５

０Ｂに格納されているセッション鍵はＫｓ２ａであるが、表記の関係上、ログメモリ２５０Ｂから取得したセッション鍵をＫｓ２ｃとしている。そして、コントローラ２１４は、取得したセッション鍵Ｋｓ２ｃをバスＢＳ３を介して暗号処理部２２４へ出力する。

【０１４４】

暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ｂによって、バスＢＳ３から取得したセッション鍵Ｋｓ２ｃを暗号化し、Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）生成する（ステップＳ１１９）。そして、暗号処理部２２４は、生成したＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）をバスＢＳ３に出力する。バスＢＳ３に出力されたＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）は、コントローラ２１４により受理され、コントローラ２１４は、ステップＳ１１８において取得したデータとともに１つのデータ列ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２を生成し、ハッシュ関数を用いてハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を生成する（ステップＳ１２０）。そして、コントローラ２１４は、ハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）をバスＢＳ３を介して暗号処理部２２４へ出力する。

【０１４５】

暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ｂによって、バスＢＳ３から取得したハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を暗号化し、Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））生成する（ステップＳ１２１）。そして、暗号処理部２２４は、生成したＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））をバスＢＳ３に出力する。ここで、データ列ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２を受信ログと称し、Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））は、受信ログに対してセッション鍵Ｋｓ１ｂを用いて電子署名を行なった署名データである。また、ログメモリ２５０Ｂに格納されていたセッション鍵Ｋｓ２ｃをセッション鍵Ｋｓ１

ｂを用いて暗号化するのは、セッション鍵Ｋｓ２ｃの漏洩によるライセンスの流出の危険性を排除するためである。

【０１４６】

コントローラ２１４は、バスＢＳ３から署名データを受理すると、ステップＳ１１８において取得した受信ログを用いて、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を生成し、ＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ１２２）。

【０１４７】

端末装置１０は、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））をＨＤ２０から受理すると（ステップＳ１２３）、受理したデータをネットワーク３０を介してライセンス提供装置４０へ出力する（ステップＳ１２４）。そして、ライセンス提供装置４０は、ネットワーク３０を介して署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を受信する。（ステップＳ１２５）

図１１を参照して、ライセンス提供装置４０は、受信した署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））の検証を行なう（ステップＳ１２６）。検証処理は次のように行なわれる。

【０１４８】

配信制御部４１２は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を復号処理部４２２へ出力するとともに、セッション鍵発生部４１４にセッション鍵Ｋｓ１ｂを発生するように指示する。そして、復号処理部４２２は、セッション鍵Ｋｓ１ｂによって署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）

）を復号する。一方、配信制御部４１２は、署名付き受信ログの前半部である受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２のハッシュ値を演算し、復号処理部４２２により復号されたＨ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）の値と比較する。配信制御部４１２は、復号処理部４２２における復号処理結果から、上記の復号ができ、かつ、ハッシュ値が一致したと判断すると、ＨＤ２０から受理したデータ列は、正当なデータを含むものとしてライセンス提供装置４０において認証される。

【０１４９】

ステップＳ１２６においてＨＤ２０から受理した署名付き受信ログが認証されると、配信制御部４１２は、受理したライセンスＩＤ（ＬＩＤ）に基づいてログＤＢ４０４を検索する（ステップＳ１２７）。配信制御部４１２は、受理したライセンスＩＤ（ＬＩＤ）がログＤＢ４０４内に格納されており、ＨＤ２０に対して確かに提供を行なったライセンスであると判断すると、受理したステータスＳＴ１，ＳＴ２の内容を確認する（ステップＳ１２８）。

【０１５０】

配信制御部４１２は、ステータスＳＴ１が「受信待」であり、ステータスＳＴ２が「データ無」であるとき、ＨＤ２０に送信したはずのライセンスＬＩＣが何らかの異常によりＨＤ２０において受理されていないと判断し、受信したデータ列に含まれる暗号化データＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）を復号処理部４２２へ出力してセッション鍵Ｋｓ１ｂによってセッション鍵Ｋｓ２ｃを復号する。そして、復号されたセッション鍵Ｋｓ２ｃは、バスＢＳ１を介して配信制御部４１２へ出力され、配信制御部４１２においてセッション鍵Ｋｓ２ｃが受理される（ステップＳ１２９）。

【０１５１】

そして、配信制御部４１２は、異常発生時のセッション鍵Ｋｓ２ａを今回受理したセッション鍵Ｋｓ２ｃと比較チェックする（ステップＳ１３０）。配信制御部４１２は、セッション鍵Ｋｓ２ａとセッション鍵Ｋｓ２ｃとが一致していると判断すると、ライセンスＬＩＣの再書込に対する許可通知を端末装置１０へ出力する（ステップＳ１３３）。

【０１５２】

一方、ステップＳ１２６においてＨＤ２０から受理したデータ列が認証されなかったとき、ステップＳ１２７においてＨＤ２０から受理したライセンスＩＤ（ＬＩＤ）がログＤＢ４０４内に格納されておらず、ＨＤ２０に対して提供を行なったライセンスであると判断できないとき、ステップＳ１２８において、ＨＤ２０においてライセンスＬＩＣが受理されたものと判断されたとき、またはステップＳ１３０において、セッション鍵Ｋｓ２ａがセッション鍵Ｋｓ２ｃと一致しないと判断されたときは、配信制御部４１２は、バスＢＳ１および通信装置４５０を介してエラー通知を出力し（ステップＳ１３１）、端末装置１０は、ネットワーク３０を介してエラー通知を受理すると（ステップＳ１３２）、処理が終了する。すなわち、ライセンス提供装置４０において、ライセンスの再書込が拒否されて処理が終了する。

【０１５３】

端末装置１０のコントローラ１０８は、ステップＳ１３３においてライセンス提供装置４０が出力した許可通知を受理すると（ステップＳ１３４）、ＨＤ２０において配信動作時に生成されるセッション鍵の生成の要求通知をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する（ステップＳ１３５）。

【０１５４】

ＨＤ２０は、ライセンス提供装置４０からの再書込処理許可通知に基づいて、端末装置１０からセッション鍵の生成要求通知を受理すると、以下、図８および図９において説明したステップＳ１９から処理終了までの一連の処理において、セッション鍵Ｋｓ２ａに代えて新たなセッション鍵Ｋｓ２ｂが生成され、そのセッション鍵Ｋｓ２ｂが使用されるほかは、同様の処理が行なわれる。したがって、ステップＳ１３５に続く一連の処理の説明は繰返しになるので省略する。

【０１５５】

なお、図１０～図１２のフローチャートに示されるライセンスの配信における再書込処理中の中断に対しては、ステップＳ１０１～Ｓ１３１、ステップＳ１３３およびステップＳ１４２～Ｓ１６０のいずれかのステップにおいて処理が中断

した場合には、再び図１０～図１２のフローチャートにしたがって再書込処理を行なうことができる。一方、ステップＳ１３４～Ｓ１４１のいずれかのステップにおいて処理が中断した場合には、図８および図９のフローチャートに示されるライセンスの配信処理を最初から行なうことによって、処理を再開することができる。

【０１５６】

このようにして、端末装置１０に装着されたＨＤ２０が正規のクラス証明書Ｃｍ１を保持する機器であることを確認したうえで、クラス証明書Ｃｍ１に含まれて送信されたクラス公開鍵ＫＰｃｍ１によってライセンス提供装置４０およびＨＤ２０でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができる。これによって、不正なハードディスクへのライセンスの配信を禁止することができ、データ配信システムのセキュリティを向上させることができる。

【０１５７】

さらに、ライセンスの配信処理が中断しても、受信側のデータ記憶装置であるＨＤ２０における受信ログをライセンス提供装置４０へ送信することで、ライセンスの重複配信を行なうことなく、ライセンスの再送処理を安全に行なうことができる。

【０１５８】

その上、ＨＤ２０においてライセンスを記憶するＬＢＡの指示がなされた場合において、そのＬＢＡをログの一部として記録することによって、配信セッション中に異常が発生したとき、ログメモリ２５０Ｂに格納されたＬＢＡにしたがって、そのセッションによって記録されるべきライセンスＬＩＣのセキュアデータメモリ２５０Ａにおける記憶状態を、相当数のライセンスを記録できるセキュアデータメモリ２５０Ａ内の検索を行なうことなく、直接的にチェックすることができ、迅速に受信ログが生成される。したがって、配信処理において迅速な再書込処理を行なうことができる。

【０１５９】

［複製・移動］

図１３は、ライセンスの複製・移動が行なわれるシステムの構成を概念的に示した概略図である。図１３を参照して、端末装置１０にデータ記憶装置として２台のハードディスクＨＤ２０，ＨＤ２１が装着可能であり、端末装置１０を介してＨＤ２０からＨＤ２１へライセンスの複製または移動が行なわれる。

【０１６０】

ここで、ＨＤ２１は、ＨＤ２０と異なるデータ記憶装置であるため、ＨＤ２０とは異なる個別公開鍵ＫＰｏｍ５と個別秘密鍵Ｋｏｍ５とを保持している。この場合、ＨＤ２１における識別子ｚは、ＨＤ２０のｚ＝２とは異なるｚ＝５となる。また、ＨＤ２１のクラスは、ＨＤ２０のクラスと同じｙ＝１として以下説明する。すなわち、ＨＤ２０、ＨＤ２１とも、クラス証明書Ｃｍ１＝ＫＰｃｍ１／／Ｉｃｍ１／／Ｅ（Ｋａ，ＫＰｃｍ１／／Ｉｃｍ１）およびクラス秘密鍵Ｋｃｍ１を保持する。しかしながら、ＨＤ２１のクラスがＨＤ２０のクラスと異なる（ｙ≠１）場合には、クラス証明書およびクラス秘密鍵も、個別公開鍵および個別秘密鍵と同様に、ＨＤ２０とは異なったものとなる。

【０１６１】

図１４および図１５は、図１３に示すライセンスの複製・移動が可能なシステムにおいて、端末装置１０のユーザが端末装置１０から暗号化コンテンツデータのライセンスの複製または移動のリクエストを行なうことにより、端末装置１０を介して端末装置１０に装着されたＨＤ２０からＨＤ２１へライセンスの複製または移動が行なわれる際の処理（複製・移動セッション）を説明するための第１および第２のフローチャートである。

【０１６２】

図１４を参照して、端末装置１０のユーザから所望のコンテンツデータのライセンスに対する複製または移動の要求が発せられると、端末装置１０のコントローラ１０８は、バスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２１へクラス証明書の出力要求を出力する（ステップＳ２０１）。ＨＤ２１のコントローラ２１４は、端子２１０およびＡＴＡインタフェース部２１２を介してク

ラス証明書の出力要求を受理すると（ステップＳ２０２）、認証データ保持部２０２からクラス証明書Ｃｍ１＝ＫＰｃｍ１／／Ｉｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を読出し、クラス証明書Ｃｍ１をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ２０３）。

【０１６３】

端末装置１０は、ＨＤ２１からクラス証明書Ｃｍ１を受理すると（ステップＳ２０４）、受理したクラス証明書Ｃｍ１をＨＤ２０へ送信する（ステップＳ２０５）。

【０１６４】

ＨＤ２０では、端末装置１０からＨＤ２１のクラス証明書Ｃｍ１を受理すると（ステップＳ２０６）、受理したＨＤ２１のクラス証明書Ｃｍ１が正当なクラス証明書であるか否かを検証する（ステップＳ２０７）。検証処理は次のように行なわれる。

【０１６５】

ＨＤ２０は、ＨＤ２１のクラス証明書Ｃｍ１＝ＫＰｃｍ１／／Ｉｃｍ１／／Ｅ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））を受理すると、ＨＤ２１のクラス証明書Ｃｍ１に含まれる署名データＥ（Ｋａ，Ｈ（ＫＰｃｍ１／／Ｉｃｍ１））をＨＤ２０の認証部２２０において認証鍵ＫＰａで復号する。そして、認証部２２０は、さらに、クラス証明書Ｃｍ１に含まれるＫＰｃｍ１／／Ｉｃｍ１のハッシュ値を演算し、認証部２２０において復号されたＨ（ＫＰｃｍ１／／Ｉｃｍ１）の値と比較する。ＨＤ２０のコントローラ２１４は、認証部２２０における復号処理結果から、上記の復号ができ、かつ、ハッシュ値の値が一致したと判断すると、ＨＤ２１から受理したクラス証明書Ｃｍ１は、正当な証明書であると判断する。

【０１６６】

ステップＳ２０７において、ＨＤ２１のクラス証明書Ｃｍ１が正当な証明書であると判断されると、ＨＤ２０のコントローラ２１４は、ＨＤ２１のクラス証明書Ｃｍ１を承認してＨＤ２１のクラス証明書Ｃｍ１に含まれるＨＤ２１のクラス

公開鍵ＫＰｃｍ１を受理し、受理したＨＤ２１のクラス公開鍵ＫＰｃｍ１をＨＤ２０のセキュアデータ記憶部２５０内のログメモリ２５０Ｂに格納する（ステップＳ２０８）。そして、次の処理（ステップＳ２０９）へ移行する。コントローラ２１４は、正当なＨＤ２１のクラス証明書でない場合には、ＨＤ２１のクラス証明書Ｃｍ１を非承認として受理せず、エラー通知を端末装置１０へ出力する（図１５のステップＳ２５２）。そして、端末装置１０においてエラー通知が受理されると（図１５のステップＳ２５３）、配信セッションが終了する。

【０１６７】

ステップＳ２０７における検証の結果、ＨＤ２０において、ＨＤ２１が正当なクラス証明書を持つハードディスクであることが確認され、ステップＳ２０８においてＨＤ２１のクラス公開鍵ＫＰｃｍ１が受理されると、ＨＤ２０のセッション鍵発生部２２６は、セッション鍵Ｋｓ１ａを生成する（ステップＳ２０９）。セッション鍵Ｋｓ１ａは、認証部２２０によって得られたＨＤ２１のクラス公開鍵ＫＰｃｍ１によって、暗号処理部２２２において暗号化され、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ａ）が生成される（ステップＳ２１０）。

【０１６８】

そして、コントローラ２１４は、ライセンスＩＤ（ＬＩＤ）および暗号化されたセッション鍵Ｋｓ１ａを１つのデータ列ＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）として、ＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ２１１）。

【０１６９】

ここで、ライセンスＩＤ（ＬＩＤ）は、事前に管理ファイルを参照することでＨＤ２０のコントローラ２１４が取得している。管理ファイルは、ＨＤ２０に記憶されている暗号化コンテンツデータとライセンスとの関係を管理するための管理データを記録したデータファイルであって、ノーマルデータ記憶部２７０に記憶され、暗号化コンテンツデータの記録消去や、ライセンスの書込、移動および消去によってその内容が更新される。

【０１７０】

端末装置１０は、ＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受理すると（ステ

ップＳ２１２）、受理したＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）をＨＤ２１へ出力する（ステップＳ２１３）。そして、ＨＤ２１のコントローラ２１４は、端子２１０およびＡＴＡインタフェース部２１２を介してＬＩＤ／／Ｅ（ＫＰｃｍ１，Ｋｓ１ａ）を受理する（ステップＳ２１４）。続いて、コントローラ２１４は、バスＢＳ３を介してＥ（ＫＰｃｍ１，Ｋｓ１ａ）を復号処理部２３０へ与え、復号処理部２３０は、Ｋｃｍ保持部２０４に保持されるＨＤ２１に固有なクラス秘密鍵Ｋｃｍ１によって復号処理することにより、セッション鍵Ｋｓ１ａを復号し、セッション鍵Ｋｓ１ａを受理する（ステップＳ２１５）。

【０１７１】

ＨＤ２１のコントローラ２１４は、ＨＤ２０で生成されたセッション鍵Ｋｓ１ａの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０は、ＨＤ２１においてセッション鍵Ｋｓ１ａが受理された旨の通知を受理すると、ＨＤ２１において複製・移動動作時に生成されるセッション鍵の生成の要求通知をＨＤ２１へ出力する（ステップＳ２１６）。ＨＤ２１のコントローラ２１４は、端子２１０およびＡＴＡコントローラ２１２を介してセッション鍵の生成要求通知を受理すると、セッション鍵発生部２２６に対してライセンスの複製・移動時に生成されるセッション鍵の生成を指示する。そして、セッション鍵発生部２２６は、セッション鍵Ｋｓ２ａを生成する（ステップＳ２１７）。

【０１７２】

セッション鍵発生部２２６は、セッション鍵Ｋｓ２ａを生成すると、バスＢＳ３を介してコントローラ２１４へ出力し、セッション鍵Ｋｓ２ａを受けたコントローラ２１４は、ステップＳ２１４において受理したライセンスＩＤ（ＬＩＤ）とセッション鍵Ｋｓ２ａとをＨＤ２１のセキュアデータ記憶部２５０内のログメモリ２５０Ｂへ格納し、ステータスＳＴ１を「受信待」にする（ステップＳ２１８）。

【０１７３】

続いて、ＨＤ２１の暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ａによって、切換スイ

ッチ２６２の接点ＰｄとＰｆとを順に切換えることによって与えられるセッション鍵Ｋｓ２ａと個別公開鍵ＫＰｏｍ５とからなる１つのデータ列を暗号化し、Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）を生成する（ステップＳ２１９）。そして、暗号処理部２２４は、Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）をバスＢＳ３に出力する。バスＢＳ３に出力された暗号化データＥ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）は、コントローラ２１４により受理され、コントローラ２１４は、受理した暗号化データとライセンスＩＤ（ＬＩＤ）とを１つのデータ列としたデータＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）をＡＴＡインタフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ２２０）。

【０１７４】

そして、端末装置１０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）をＨＤ２１から受理すると（ステップＳ２２１）、受理したデータをＨＤ２０へ出力する（ステップＳ２２２）。

【０１７５】

ＨＤ２０は、データＬＩＤ／／Ｅ（Ｋｓ１ａ，Ｋｓ２ａ／／ＫＰｏｍ５）を受理すると（ステップＳ２２３）、復号処理部２２８においてセッション鍵Ｋｓ１ａによる復号処理を実行し、ＨＤ２１で生成されたセッション鍵Ｋｓ２ａ、およびＨＤ２１の個別公開鍵ＫＰｏｍ５を受理する（ステップＳ２２４）。そして、復号処理部２２８は、復号したセッション鍵Ｋｓ２ａをバスＢＳ３を介してコントローラ２１４へ出力し、コントローラ２１４は、ステップＳ２２３において受理したライセンスＩＤ（ＬＩＤ）とセッション鍵Ｋｓ２ａとをＨＤ２０のセキュアデータ記憶部２５０内のログメモリ２５０Ｂへ格納し、ステータスＳＴ１を「送信待」にする（ステップＳ２２５）。

【０１７６】

ステップＳ２２５の処理を終えると、ＨＤ２０のコントローラ２１４は、その旨をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して、ＨＤ２０からの通知を受理すると、ＨＤ２０のセ

キュアデータ記憶部２５０において、ＨＤ２０からＨＤ２１へ送信するライセンスＬＩＣが格納されているＬＢＡをバスＢＳ２およびＨＤインターフェース１１０を介してＨＤ２０へ出力する（ステップＳ２２６）。ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介して送信対象のライセンスＬＩＣの格納先ＬＢＡを受理すると（ステップＳ２２７）、その受理したＬＢＡをセキュアデータ記憶部２５０のログメモリ２５０Ｂに記憶する（ステップＳ２２８）。

【０１７７】

そして、コントローラ２１４は、受理したＬＢＡに格納されるライセンスＬＩＣに対応する有効フラグメモリ２５０Ｃのフラグが「有効」であるか「無効」であるかを確認する（ステップＳ２２９）。コントローラ２１４は、有効フラグが「有効」であると、受理したＬＢＡに基づいて、そのＬＢＡに格納されるライセンスＬＩＣを取得する（ステップＳ２３０）。

【０１７８】

図１５を参照して、コントローラ２１４は、対象のライセンスＬＩＣを取得すると、ライセンスＬＩＣに含まれるライセンスＩＤ（ＬＩＤ）と、ステップＳ２２３において受理したライセンスＩＤ（ＬＩＤ）とを比較し、一致しているか否かをチェックする（ステップＳ２３１）。コントローラ２１４は、一致していると判断すると、取得したライセンスＬＩＣに含まれる制御情報ＡＣを確認して利用制限がかけられていないかをチェックする（ステップＳ２３２）。

【０１７９】

コントローラ２１４は、制御情報ＡＣにおいてライセンスＬＩＣの利用が禁止されていないことを確認すると、取得したライセンスＬＩＣを暗号処理部２３２に与える。暗号処理部２３２は、復号処理部２２８によって得られたＨＤ２１の個別公開鍵ＫＰｏｍ５によってライセンスＬＩＣを暗号化して暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）を生成する（ステップＳ２３３）。そして、暗号処理部２３２は、暗号化データＥ（ＫＰｏｍ５，ＬＩＣ）を切替スイッチＰｃを介して暗号処理部２２４へ出力し、暗号処理部２２４は、暗号処理部２３２から受けた暗号化データを復号処理部２２８から受けたセッション鍵Ｋｓ２ａによって暗号化

し、暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を生成する（ステップＳ２３４）。

【０１８０】

続いて、コントローラ２１４は、対象のライセンスＬＩＣに含まれる制御情報ＡＣに基づいて、ＨＤ２０からＨＤ２１へのライセンスＬＩＣの送信が「移動」であるか「複製」であるかを確認する（ステップＳ２３５）。コントローラ２１４は、「移動」であると確認したときは、その対象のライセンスＬＩＣに対応する有効フラグメモリ２５０Ｃのフラグを「無効」に変更する（ステップＳ２３６）。一方、コントローラ２１４は、「複製」であると確認したときには、当該ライセンスＬＩＣがＨＤ２０に残っていてもよいので、有効フラグメモリ２５０Ｃのフラグの変更は行なわずに次の処理（ステップＳ２３７）へ移行する。

【０１８１】

コントローラ２１４は、有効フラグメモリ２５０Ｃの処理が終わると、ログメモリ２５０ＢのステータスＳＴ１を「送信済」に変更し（ステップＳ２３７）、ＡＴＡインタフェース部２１２および端子２１０を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を端末装置１０へ送信する（ステップＳ２３８）。

【０１８２】

一方、ステップＳ２２９において受理したＬＢＡに対応する有効フラグメモリ２５０Ｃのフラグが「無効」であったとき、ステップＳ２３１においてライセンスＩＤ（ＬＩＤ）が一致しないとき、または、ステップＳ２３２において、取得したライセンスＬＩＣに含まれる制御情報ＡＣにより当該ライセンスＬＩＣの利用が禁止されているときは、コントローラ２１４は、端末装置１０に対してエラー通知を出力し（ステップＳ２５２）、端末装置１０においてエラー通知が受理されると（ステップＳ２５３）、処理が終了する。

【０１８３】

端末装置１０は、ステップＳ２３８においてＨＤ２０から出力された暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を受理すると（ステップＳ２３９）、受理した暗号化データをＨＤ２１へ出力する（ステップＳ２４０）。ＨＤ

２１のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介して暗号化データＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を受理すると（ステップＳ２４１）、バスＢＳ３へ出力する。復号処理部２２８は、セッション鍵発生部２２６から与えられたセッション鍵Ｋｓ２ａを用いてバスＢＳ３に出力されたデータＥ（Ｋｓ２ａ，Ｅ（ＫＰｏｍ５，ＬＩＣ））を復号し、ＨＤ２１において、ライセンスＬＩＣが個別公開鍵ＫＰｏｍ５により暗号化された暗号化ライセンスＥ（ＫＰｏｍ５，ＬＩＣ）が受理される（ステップＳ２４２）。そして、復号処理部２２８は、暗号化ライセンスＥ（ＫＰｏｍ５，ＬＩＣ）をバスＢＳ３へ出力する。

【０１８４】

コントローラ２１４の指示によって、暗号化ライセンスＥ（ＫＰｏｍ５，ＬＩＣ）は、復号処理部２１６において個別秘密鍵Ｋｏｍ５によって復号され、ＨＤ２１においてライセンスＬＩＣが受理される（ステップＳ２４３）。

【０１８５】

コントローラ２１４は、ライセンスＬＩＣの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介して、ＨＤ２１においてライセンスＬＩＣが受理された旨の通知を受理すると、ＨＤ２１のセキュアデータ記憶部２５０において、その受信したライセンスＬＩＣを格納するＬＢＡをバスＢＳ２およびＨＤインターフェース１１０を介してＨＤ２１へ出力する（ステップＳ２４４）。ＨＤ２１のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介してライセンスＬＩＣの格納先のＬＢＡを受理すると（ステップＳ２４５）、その受理したＬＢＡをログメモリ２５０Ｂに記憶する（ステップＳ２４６）。

【０１８６】

そして、コントローラ２１４は、受理したライセンスＬＩＣに含まれるライセンスＩＤ（ＬＩＤ）と、ステップＳ２１４において受理したライセンスＬＩＤ（ＬＩＤ）とを比較し、一致しているか否かをチェックする（ステップＳ２４７）。コントローラ２１４は、ＬＩＤが一致しており、受理したライセンスＬＩＣが

正しいものであると判断すると、端末装置１０から受理したセキュアデータ記憶部２５０内のＬＢＡに、受理したライセンスＬＩＣを記憶する（ステップＳ２４８）。

【０１８７】

コントローラ２１４は、指定されたＬＢＡにライセンスＬＩＣを記憶すると、有効フラグメモリ２５０Ｃのそのに対応するフラグを「有効」にする（ステップＳ２４９）。そして、コントローラ２１４は、さらに、ログメモリ２５０Ｂのステータスｓｔ１を「受信済」にし（ステップＳ２５０）、複製・移動セッションにおける一連の処理が終了したことをＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０に通知する。

【０１８８】

そして、端末装置１０において、ＨＤ２１からの処理終了通知が受理されると、ＨＤ２０およびＨＤ２１間の複製・移動セッションが正常終了する。

【０１８９】

一方、ステップＳ２４７において、コントローラ２１４は、ＬＩＤが一致しておらず、受理したライセンスＬＩＣが正しくないと判断すると、ＡＴＡインターフェース部２１２および端子２１０を介してエラー通知を端末装置１０へ出力し（ステップＳ２５１）、端末装置１０においてエラー通知が受理されると（ステップＳ２５３）、複製・移動セッションが終了する。

【０１９０】

ここで、配信セッションのときと同様に、図１４および図１５に示された複製・移動セッションにおける一連の処理において、ステップＳ２２７からステップＳ２５２の処理中に異常が発生し、処理が中断したときは、再書込処理の対象となる。

【０１９１】

ここで、図１４および図１５に示された複製・移動セッションにおいて、ステップＳ２２７からステップＳ２３５までの処理を再書込処理の対象としたのは、この一連の処理がＨＤ２０の内部処理であり、ステップＳ２２６の終了後は、ステップＳ２３８まで端末装置１０においていずれのステップを処理中に処理が中

断したかを特定できないため、すべてステップＳ２３６が実行されてライセンスが無効化されたものとし、必ず再書込処理の対象としたものである。

【０１９２】

そして、ステップＳ２３６からステップＳ２４７までの処理を再書込処理の対象としたのは、移動処理の場合、この間は、ＨＤ２０内のライセンスがステップＳ２３６において無効化され、かつ、ＨＤ２１内に有効なライセンスが格納されていない状態であって、この間に処理が中断すると、対象となるライセンスが消失してしまうからである。なお、複製処理の場合は、ステップＳ２３６においてライセンスは無効化されないため、移動の場合と同様に再書込処理を行なうようにしても、また、複製処理を最初から行なうようにしてもよい。しかしながら、移動処理の場合は、再書込処理によってのみしかライセンスを復活させることはできない。

【０１９３】

また、ステップＳ２４８からステップＳ２５０までの処理を再書込処理の対象としたのは、ステップＳ２４９，Ｓ２５０については、これらの処理はステップＳ２４８におけるライセンス書込後の処理であるから本来は処理が終了しているところ、端末装置１０からはステップＳ２４８の終了が特定できないため、ステップＳ２４８が終了していないものとみなして、ステップＳ２４８からステップＳ２５０を再書込処理の対象としたものである。なお、ステップＳ２４８が終了していて再書込処理が行なわれた場合には、再書込処理において再書込は拒否される。

【０１９４】

また、ステップＳ２５１の処理を再書込処理の対象としたのは、本来この処理で処理が中断するのはかなり特殊な場合に限られるものであるが、端末装置１０においては、ステップＳ２５１において処理が中断したことを特定することができないため、再書込処理の対象としたものである。

【０１９５】

なお、端末装置１０において、上述したように当該セッションがライセンスの複製であると判断できる場合、あるいはステップＳ２２７からステップＳ２３５

およびステップＳ２４９からステップＳ２５１のいずれかのステップで処理が中断したかを特定できる場合においては、必ずしも再書込処理とする必要はなく、図１４および図１５に示された複製・移動セッションを再度実行すればよい。

【０１９６】

図１６から図１８は、図１４および図１５において示した複製・移動セッションの処理フローにおけるステップＳ２２７からステップＳ２５２の処理中に異常が発生したときに行なわれる再書込処理の第１から第３のフローチャートである。

【０１９７】

図１６を参照して、端末装置１０は、ステップＳ２２７からステップＳ２５２の処理中に異常が発生したと判断すると、ライセンスＬＩＣの再送要求をＨＤ２０へ出力する（ステップＳ３０１）。ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介して再送要求を受理すると、セキュアデータ記憶部２５０内のログメモリ２５０Ｂに格納されているステータスＳＴ１の状態を確認する（ステップＳ３０２）。コントローラ２１４は、ステータスＳＴ１が「送信待」または「送信済」でないとき、すなわち複製・移動セッションにおいてライセンスＬＩＣの送信側でないときは、図１８に示すステップＳ３７１へ処理が移行する。

【０１９８】

ＨＤ２０のコントローラ２１４は、ステータスＳＴ１が「送信待」または「送信済」であるときは、セッション鍵発生部２２６にセッション鍵を生成するように指示し、セッション鍵発生部２２６は、セッション鍵Ｋｓ１ａを生成する（ステップＳ３０３）。セッション鍵Ｋｓ１ｂが生成されると、コントローラ２１４は、中断以前に受理してログメモリ２５０Ｂに格納されたＨＤ２１のクラス公開鍵ＫＰｃｍ１を取得する（ステップＳ３０４）。そして、そのＨＤ２１のクラス公開鍵ＫＰｃｍ１によって、セッション鍵Ｋｓ１ｂが暗号処理部２２２によって暗号化され、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）が生成される（ステップＳ３０５）。コントローラ２１４は、生成された暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）をＡＴＡインターフェース部２１２および端子２１０を介して端末装

置１０へ出力する（ステップＳ３０６）。

【０１９９】

端末装置１０は、暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ｂ）を受理すると（ステップＳ３０７）、受理した暗号化データＥ（ＫＰｃｍ１，Ｋｓ１ａ）をＨＤ２１へ出力する（ステップＳ３０８）。ＨＤ２１のコントローラ２１４は、端子２１０およびＡＴＡインタフェース部２１２を介してＥ（ＫＰｃｍ１，Ｋｓ１ａ）を受理すると（ステップＳ３０９）、バスＢＳ３を介してＥ（ＫＰｃｍ１，Ｋｓ１ａ）を復号処理部２３０へ与える。そうすると、復号処理部２３０は、Ｋｃｍ保持部２０４に保持されるＨＤ２１に固有なクラス秘密鍵Ｋｃｍ１によって復号処理を実行してセッション鍵Ｋｓ１ｂを復号し、セッション鍵Ｋｓ１ｂを受理する（ステップＳ３１０）。

【０２００】

ＨＤ２１のコントローラ２１４は、ＨＤ２０で生成されたセッション鍵Ｋｓ１ｂの受理を確認すると、ＡＴＡインターフェース部２１２および端子２１０を介してその旨を端末装置１０に通知する。端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介してＨＤ２１からの通知を受理すると、ＨＤ２１のログメモリ２５０Ｂに格納されるログのＨＤ２０への出力要求をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２１へ出力する（ステップＳ３１１）。ＨＤ２１のコントローラ２１４は、端子２１０およびＡＴＡコントローラ２１２を介してログの出力要求通知を受理すると（ステップＳ３１２）、ログメモリ２５０Ｂに格納されたＬＢＡに記憶されるライセンスＬＩＣのライセンスＩＤ（ＬＩＤ）と、ログメモリ２５０Ｂに格納されたライセンスＩＤ（ＬＩＤ）とが一致するか否かを確認する（ステップＳ３１３）。

【０２０１】

コントローラ２１４は、ライセンスＩＤ（ＬＩＤ）が一致すると、さらに、ログメモリ２５０Ｂに格納されたＬＢＡに記憶されるライセンスＬＩＣに対応する有効フラグメモリ２５０Ｃのフラグを確認し、そのライセンスＬＩＣが有効であるか無効であるかを確認する（ステップＳ３１４）。コントローラ２１４は、有効フラグメモリ２５０Ｃのフラグが「有効」であるときは、ログメモリ２５０Ｂ

のステータスＳＴ２を「データ有」に変更し（ステップＳ３１５）、次の処理（ステップＳ３１８）へ移行する。一方、コントローラ２１４は、有効フラグメモリ２５０Ｃのフラグが「無効」であるときは、ログメモリ２５０Ｂのステータス ＳＴ２を「移動済」に変更し（ステップＳ３１６）、次の処理（ステップＳ３１８）へ移行する。

【０２０２】

また、コントローラ２１４は、ステップＳ３１３において両ライセンスＩＤ（ＬＩＤ）が一致しないときは、ログメモリ２５０ＢのステータスＳＴ２を「データ無」に変更する（ステップＳ３１７）。

【０２０３】

このように、複製・移動セッションにおいても、ログメモリ２５０Ｂに格納されたＬＢＡを用いて、そのＬＢＡにより指定されるセキュアデータメモリ２５０Ａの記憶位置に記憶されるライセンスのライセンスＩＤ（ＬＩＤ）をＬＢＡに基づいて直接確認できるので、セキュアデータメモリ２５０Ａに相当数のライセンスが格納されているときであっても、それらのライセンスを逐一検索することなしにライセンスＩＤ（ＬＩＤ）の特定または有無を判断することができる。

【０２０４】

ステータスＳＴ２の変更処理がなされると、コントローラ２１４は、ログメモリ２５０Ｂからライセンス ＩＤ（ＬＩＤ）、ステータスＳＴ１，ＳＴ２およびセッション鍵Ｋｓ２ｃを取得する（ステップＳ３１８）。ここで、ログメモリ２５０Ｂに格納されているセッション鍵はＫｓ２ａであるが、表記の関係上、ログメモリ２５０Ｂから取得したセッション鍵をＫｓ２ｃとしている。そして、コントローラ２１４は、取得したセッション鍵Ｋｓ２ｃをバスＢＳ３を介して暗号処理部２２４へ出力する。

【０２０５】

暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ｂによってセッション鍵Ｋｓ２ｃを暗号化し、Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）生成する（ステップＳ３１９）。そして、暗号処理部２２４は、生成したＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）をバスＢＳ３に出力する。バ

スＢＳ３に出力されたＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）は、コントローラ２１４により受理され、コントローラ２１４は、ステップＳ３１８において取得したデータとともに１つの受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２を生成し、そのハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を生成する（ステップＳ３２０）。そして、コントローラ２１４は、ハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）をバスＢＳ３を介して暗号処理部２２４へ出力する。

【０２０６】

暗号処理部２２４は、切換スイッチ２６０の接点Ｐｂを介して復号処理部２３０より与えられるセッション鍵Ｋｓ１ｂによって、バスＢＳ３から取得したハッシュ値Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）を暗号化し、署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））生成する（ステップＳ３２１）。そして、暗号処理部２２４は、生成したＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））をバスＢＳ３に出力する。

【０２０７】

コントローラ２１４は、バスＢＳ３から署名データを取得すると、ステップＳ３１８において取得した受信ログを用いて、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を生成し、ＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ３２２）。

【０２０８】

端末装置１０は、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））をＨＤ２１から受理すると（ステップＳ３２３）、受理したデータをＨＤ２０へ出力する（ステップＳ３２４）。

【０２０９】

ＨＤ２０は、署名付き受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ

１／／ＳＴ２／／Ｅ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を受理すると（ステップＳ３２５）、受理したデータの検証を行なう（ステップＳ３２６）。検証処理は、以下のように行われる。

【０２１０】

ＨＤ２０のコントローラ２１４は、署名付き受信ログを受理すると、まず、受理した署名付き受信ログの後半部である署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を復号処理部２２８へ出力するとともに、セッション鍵発生部２２６にセッション鍵Ｋｓ１ｂを発生するように指示する。そして、復号処理部２２８は、セッション鍵Ｋｓ１ｂによって署名データＥ（Ｋｓ１ｂ，Ｈ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２））を復号する。一方、ＨＤ２０のコントローラ２１４は、署名付き受信ログの前半部である受信ログＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２のハッシュ値を演算し、復号処理部２２８により復号されたＨ（ＬＩＤ／／Ｅ（Ｋｓ１ｂ，Ｋｓ２ｃ）／／ＳＴ１／／ＳＴ２）の値と比較する。ＨＤ２０のコントローラ２１４は、復号処理部２２８における復号処理結果から、上記の復号ができ、かつ、ハッシュ値が一致したと判断すると、ＨＤ２１から受理したデータ列は、正当なデータを含むものとしてＨＤ２０において認証される。

【０２１１】

ステップＳ３２６において署名付き受信ログの検証が行なわれ、そのデータがＨＤ２０において承認されると、ＨＤ２０のコントローラ２１４は、ステップＳ３２５において受理したデータに含まれるライセンスＩＤ（ＬＩＤ）をログメモリ２５０Ｂに格納されるライセンスＩＤ（ＬＩＤ）と比較する（ステップＳ３２７）。

【０２１２】

コントローラ２１４は、ライセンスＩＤ（ＬＩＤ）が一致すると、受信したデータ列に含まれる暗号データＥ（Ｋｓ１ｂ，Ｋｓ２ｃ）を復号処理部２２８へ出力し、復号処理部２２８は、セッション鍵発生部２２６から受けるセッション鍵Ｋｓ１ｂによってセッション鍵Ｋｓ２ｃを復号し、セッション鍵Ｋｓ２ｃが受理

される（ステップＳ３２８）。そして、復号されたセッション鍵Ｋｓ２ｃは、バスＢＳ３を介してコントローラ２１４へ出力される。続いて、コントローラ２１４は、エラー発生時のセッション鍵Ｋｓ２ａを今回受理したセッション鍵Ｋｓ２ｃと比較チェックする（ステップＳ３２９）。コントローラ２１４は、セッション鍵Ｋｓ２ａとセッション鍵Ｋｓ２ｃとが一致していると判断すると、受理したステータスＳＴ１，ＳＴ２の内容を確認する（ステップＳ３３０）。

【０２１３】

ＨＤ２０のコントローラ２１４は、受信したステータスＳＴ１が「受信待」であり、ステータスＳＴ２が「データ無」であるとき、ＨＤ２１に送信したはずのライセンスＬＩＣが何らかの異常によりＨＤ２１において受理されていないと判断する。そうすると、ＨＤ２０のコントローラ２１４は、さらに、ログメモリ２５０Ｂに格納されたＬＢＡに記憶されるライセンスＬＩＣのライセンスＩＤ（ＬＩＤ）と、ログメモリ２５０Ｂに格納されたライセンスＩＤ（ＬＩＤ）とが一致するか否かを確認する（ステップＳ３３１）。ＨＤ２０のコントローラ２１４は、ライセンスＩＤ（ＬＩＤ）が一致すると、さらに、ログメモリ２５０Ｂに格納されたＬＢＡに対応する有効フラグメモリ２５０Ｃのフラグを確認し、そのライセンスＬＩＣが有効であるか無効であるかを確認する（ステップＳ３３２）。そして、コントローラ２１４は、有効フラグメモリ２５０Ｃのフラグが「無効」であるときは、その有効フラグメモリ２５０Ｃのフラグを「有効」に変更する（ステップＳ３３３）。一方、コントローラ２１４は、有効フラグメモリ２５０Ｃのフラグが「有効」であるときは、次の処理（ステップＳ３３４）へ移行する。そして、コントローラ２１４は、ログメモリ２５０Ｂに格納されるＬＢＡを取得し、ＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ３３４）。

【０２１４】

端末装置１０のコントローラ１０８は、ＨＤ２０からＨＤインターフェース部１１０およびバスＢＳ２を介して対象のライセンスＬＩＣが格納されるＬＢＡを受理すると（ステップＳ３３５）、ＨＤ２１において複製・移動動作時に生成されるセッション鍵の生成の要求通知をバスＢＳ２およびＨＤインターフェース部

１１０を介してＨＤ２１へ出力する（ステップＳ３３６）。

【０２１５】

ＨＤ２１は、端末装置１０からセッション鍵の生成要求通知を受理すると、以下、図１４および図１５において説明したステップＳ２１７から処理終了までの一連の処理において、セッション鍵Ｋｓ２ａに代えて新たなセッション鍵Ｋｓ２ｂが生成され、そのセッション鍵Ｋｓ２ｂが使用されるほかは、同様の処理が行なわれる。したがって、ステップＳ３３６に続く一連の処理の説明は繰返しになるので省略する。

【０２１６】

なお、ステップＳ３３５において処理を終了し、ＨＤ２０にライセンスを残すことも可能である。この場合、図１４および図１５に示したフローチャートにしたがって、再度ライセンスを移動させることができる。

【０２１７】

なお、図１６～図１８のフローチャートに示されるライセンスの移動または複製における再書込処理の中断に対しては、ステップＳ３０１～Ｓ３４４およびステップＳ３４７～Ｓ３７１のいずれかのステップにおいて処理が中断した場合には、再び図１６～図１８に示されるフローチャートにしたがって再書込処理を行なうことができる。一方、ステップＳ３２５～Ｓ３４６のいずれかのステップにおいて処理が中断した場合には、図１４および図１５のフローチャートに示されるライセンスの移動または複製の処理を最初から行なうことによって、処理を再開することができる。

【０２１８】

このようにして、端末装置１０に装着された複数のハードディスク間におけるライセンスの複製または移動に関しても、複製先または移動先のＨＤ２１から受取ったクラス証明書Ｃｍ１が有効であることを確認し、クラス証明書Ｃｍ１に含まれて送信されたクラス公開鍵ＫＰｃｍ１によってライセンスの複製・移動が行なわれる複数のハードディスク間でそれぞれ生成される暗号鍵（セッション鍵）をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、不正なハードディスクへのライセンス

の複製または移動を禁止することができる。さらには、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、出力先のなりすましからライセンスを保護して、システムのセキュリティを向上させることができる。

【０２１９】

さらに、ライセンスの複製・移動セッションの中断においても、配信セッションと同様に、受信側のデータ記憶装置であるＨＤ２１における複製・移動セッションの対象となったライセンスＬＩＣに対する受信ログを送信側のデータ記憶装置であるＨＤ２０へ送信し、ＨＤ２０において、自身のログメモリ２５０Ｂに記憶される内容と、ログメモリ２５０Ｂに記憶されるＬＢＡによって特定されるセキュアデータメモリ２５０Ａに記憶されるライセンスＬＩＣとを比較し、さらに有効フラグメモリ２５０Ｃに記憶されるフラグを参照することによって、中断した複製・移動セッションがライセンスの移動を行なう処理である場合において、２つのデータ記憶装置ＨＤ２０およびＨＤ２１に利用可能なライセンスが重複して存在することのない安全な再書込処理が提供される。

【０２２０】

その上、受信側のデータ記憶装置であるＨＤ２１においてライセンスを記憶するＬＢＡの指示がなされた場合において、そのＬＢＡをログの一部として記録することによって、複製・移動セッション中に異常が発生したとき、ログメモリ２５０Ｂに格納されたＬＢＡにしたがって、そのセッションによって記録されるべきライセンスＬＩＣのセキュアデータメモリ２５０Ａにおける記憶状態を、相当数のライセンスを記録できるセキュアデータメモリ２５０Ａ内の検索を行なうことなく、直接的にチェックすることができ、迅速に受信ログが生成される。したがって、複製・移動処理においても迅速な再書込処理を行なうことができる。また、送信側のデータ記憶装置であるＨＤ２０においても、ダイレクトに処置の対象であるライセンスＬＩＣの内容および状態（利用可否）が判断できる。

【０２２１】

このように、本発明は、複製・移動セッションの中断によるライセンスＬＩＣの消失を回避し、迅速な処理を行なうことができるデータ記憶装置およびその処

理手順を提供するとともに、再書込処理に至った場合でも安全に処理が行なわれ、確実な著作権保護を実現することができるデータ記憶装置およびその処理手順を提供する。

【０２２２】

なお、図１４～図１８におけるＨＤ２１の処理ステップＳ２０２，２０３，Ｓ２１４，Ｓ２１５，Ｓ２１７～Ｓ２２０，Ｓ２４１～Ｓ２４３，Ｓ２４５～Ｓ２５１，Ｓ３０９，Ｓ３１０，Ｓ３１２～Ｓ３２２，Ｓ３３７～Ｓ３４０，Ｓ３６１～Ｓ３６３，Ｓ３６５～Ｓ３７１は、図８～図１２におけるＨＤ２０の処理ステップＳ２，Ｓ３，Ｓ１６，Ｓ１７，Ｓ１９～Ｓ２２，Ｓ３３～Ｓ３５，Ｓ３７～Ｓ４３，Ｓ１０９，Ｓ１１０，Ｓ１１２～Ｓ１２２，Ｓ１３６～Ｓ１３９，Ｓ１５０～Ｓ１５２，Ｓ１５４～Ｓ１６０とそれぞれ同じである。すなわち、ライセンスの移動または複製時におけるＨＤ２１の処理とライセンスの配信処理時におけるＨＤ２０の処理とは同じ処理であって、これらの処理は、いずれも、データ記憶装置（ＨＤ２０，ＨＤ２１）においてライセンスを書込むためのデータ記憶装置における処理である。

【０２２３】

［再生許諾］

再び図５を参照して、コンテンツデータを再生する再生回路１５０を備えた端末装置１０にデータ記憶装置としてのＨＤ２０が装着され、コンテンツデータの再生許諾は、ＨＤ２０から端末装置１０内の再生回路１５０に対して行なわれる。

【０２２４】

図１９は、端末装置１０のユーザが端末装置１０から暗号化コンテンツデータの再生リクエストを行なうことにより、端末装置１０に装着されたＨＤ２０から端末装置１０内の再生回路１５０へ再生許諾が行なわれる際の処理（再生許諾セッション）を説明するためのフローチャートである。

【０２２５】

図１９を参照して、端末装置１０のユーザから所望のコンテンツデータの再生リクエストがなされると、端末装置１０のコントローラ１０８は、バスＢＳ２を

介して再生回路１５０へクラス証明書の出力要求を出力する（ステップＳ４０１）。再生回路１５０において、認証データ保持部１５０２は、バスＢＳ２からクラス証明書の出力要求を受けると（ステップＳ４０２）、保持しているクラス証明書Ｃｐ３＝ＫＰｃｐ３／／Ｉｃｐ３／／Ｅ（Ｋａ，Ｈ（ＫＰｃｐ３／／Ｉｃｐ３））をバスＢＳ２へ出力する（ステップＳ４０３）。

【０２２６】

コントローラ１０８は、バスＢＳ２からクラス証明書Ｃｐ３を受理すると（ステップＳ４０４）、受理したクラス証明書Ｃｐ３をバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する（ステップＳ４０５）。

【０２２７】

ＨＤ２０では、端末装置１０からクラス証明書Ｃｐ３を受理すると（ステップＳ４０６）、受理したクラス証明書Ｃｐ３が正当なクラス証明書であるか否かを検証する（ステップＳ４０７）。検証処理は、複製・移動セッションにおけるステップＳ２０７において説明したのと同様の方法で行なわれ、説明は省略する。

【０２２８】

ステップＳ４０７において、クラス証明書Ｃｐ３が正当な証明書であると判断された場合、コントローラ２１４は、クラス証明書Ｃｐ３を承認し、クラス証明書Ｃｐ３に含まれるクラス公開鍵ＫＰｃｐ３を受理する（ステップＳ４０８）。そして、次の処理（ステップＳ４０９）へ移行する。コントローラ２１４は、正当なクラス証明書でない場合には、クラス証明書Ｃｐ３を非承認とし、クラス証明書Ｃｐ３を受理せずにエラー通知を端末装置１０へ出力し（ステップＳ４３５）、端末装置１０においてエラー通知が受理されると（ステップＳ４３６）、再生許諾セッションが終了する。

【０２２９】

ステップＳ４０７における検証の結果、ＨＤ２０において、再生回路１５０が正当なクラス証明書を持つ再生回路であることが確認され、ステップＳ４０８においてクラス公開鍵ＫＰｃｐ３が受理されると、ＨＤ２０のセッション鍵発生部２２６は、セッション鍵Ｋｓ１ｄを生成する（ステップＳ４０９）。セッション鍵Ｋｓ１ｄは、受理されたクラス公開鍵ＫＰｃｐ３によって、暗号処理部２２２

において暗号化され、暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）が生成される（ステップＳ４１０）。

【０２３０】

そして、コントローラ２１４は、暗号処理部２２２からバスＢＳ３を介して暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）を受けると、ＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ４１１）。

【０２３１】

端末装置１０において、ＨＤインターフェース部１１０およびバスＢＳ２を介してコントローラ１０８が暗号データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）を受理すると（ステップＳ４１２）、コントローラ１０８は、受理した暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）をバスＢＳ２を介して再生回路１５０へ出力する（ステップＳ４１３）。再生回路１５０の復号処理部１５０６は、バスＢＳ２から暗号化データＥ（ＫＰｃｐ３，Ｋｓ１ｄ）を受理すると（ステップＳ４１４）、Ｋｃｐ保持部１５０４に保持される再生回路１５０に固有なクラス秘密鍵Ｋｃｐ３によって復号処理することによりセッション鍵Ｋｓ１ｄを復号し、セッション鍵Ｋｓ１ｄが受理される（ステップＳ４１５）。

【０２３２】

セッション鍵Ｋｓ１ｄが受理されると、セッション鍵発生部１５０８は、セッション鍵Ｋｓ２ｄを生成し（ステップＳ４１６）、生成したセッション鍵Ｋｓ２ｄを暗号処理部１５１０に与える。暗号処理部１５１０は、復号処理部１５０６から受けるセッション鍵Ｋｓ１ｄをセッション鍵Ｋｓ２ｄにより暗号化し、暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を生成する（ステップＳ４１７）。そして、暗号処理部１５１０は、暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）をバスＢＳ２へ出力する（ステップＳ４１８）。

【０２３３】

コントローラ１０８は、バスＢＳ２から暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を受理し（ステップＳ４１９）、受理したデータをバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する（ステップＳ４２０）。

【０２３４】

ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介して暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を受理すると（ステップＳ４２１）、受理したデータをバスＢＳ３へ出力する。復号処理部２２８は、セッション鍵発生部２２６から与えられたセッション鍵Ｋｓ１ｄを用いてバスＢＳ３に出力された暗号化データＥ（Ｋｓ１ｄ，Ｋｓ２ｄ）を復号し、ＨＤ２０においてセッション鍵Ｋｓ２ｄが受理される（ステップＳ４２２）。そして、コントローラ２１４は、セッション鍵Ｋｓ２ｄが受理されると、その旨の通知をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する。

【０２３５】

端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスＢＳ２を介してＨＤ２０においてセッション鍵Ｋｓ２ｄが受理された旨の通知を受理すると、再生リクエストのあったコンテンツデータに対応する対象のライセンスＬＩＣが格納されているセキュアデータメモリ２５０ＡのＬＢＡをバスＢＳ２およびＨＤインターフェース部１１０を介してＨＤ２０へ出力する。

【０２３６】

ＨＤ２０のコントローラ２１４は、端子２１０およびＡＴＡインターフェース部２１２を介して対象のライセンスＬＩＣが格納されているＬＢＡを受理すると（ステップＳ４２４）、そのＬＢＡに格納されるライセンスＬＩＣに対応する有効フラグメモリ２５０Ｃのフラグが「有効」であるか「無効」であるかを確認する（ステップＳ４２５）。

【０２３７】

コントローラ２１４は、有効フラグメモリ２５０Ｃのフラグが「有効」であると、受理したＬＢＡに基づいて、対象のライセンスＬＩＣをセキュアデータメモリ２５０Ａから取得する（ステップＳ４２６）。そして、コントローラ２１４は、取得したライセンスＬＩＣに含まれる制御情報ＡＣの内容を確認する（ステップＳ４２７）。コントローラ２１４は、制御情報ＡＣにおいて利用回数が指定されているときは、制御情報ＡＣの利用回数を１増分し、次の処理（ステップＳ４

２９）へ移行する。一方、コントローラ２１４は、制御情報ＡＣにより再生制限がかけられていないときは、取得したライセンスＬＩＣに含まれるコンテンツ鍵Ｋｃをバスｂｓ３へ出力する。

【０２３８】

暗号処理部２２４は、復号処理部２２８から受けるセッション鍵Ｋｓ２ｄによりバスｂｓ３上に出力されたコンテンツ鍵Ｋｃを暗号化して暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）を生成し（ステップＳ４２９）、生成したデータをバスｂｓ３へ出力する。そして、コントローラ214は、バスｂｓ３上に出力された暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）をＡＴＡインターフェース部２１２および端子２１０を介して端末装置１０へ出力する（ステップＳ４３０）。

【０２３９】

端末装置１０のコントローラ１０８は、ＨＤインターフェース部１１０およびバスｂｓ２を介して暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）を受理すると（ステップＳ４３１）、受理したデータをバスｂｓ２へ出力する（ステップＳ４３２）。

【０２４０】

再生回路１５０の復号処理部１５１２は、バスｂｓ２から暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）を受理すると（ステップＳ４３３）、セッション鍵発生部１５０８から与えられるセッション鍵Ｋｓ２ｄを用いて暗号化データＥ（Ｋｓ２ｄ，Ｋｃ）を復号する。これにより、再生回路１５０においてコンテンツ鍵Ｋｃが受理され（ステップＳ４３４）、一連の再生許諾セッションの処理が正常終了する。

【０２４１】

一方、ステップＳ４２５において、有効フラグメモリ２５０Ｃのフラグが「無効」であったとき、またはステップＳ４２７において、制御情報ＡＣに含まれる内容が再生不可であったときは、コントローラ２１４は、端末装置１０に対してエラー通知を出力し（ステップＳ４３５）、端末装置１０においてエラー通知が受理されると（ステップＳ４３６）、再生許諾セッションが終了する。

【０２４２】

このようにして、データ記憶装置であるＨＤ２０から端末装置１０に備えられる再生回路１５０への再生許諾に関しても、再生回路１５０が正規のクラス証明

書Ｃｐ３を保持していること、およびクラス証明書Ｃｐ３に含まれて送信されたクラス公開鍵ＫＰｃｐ３が有効であることを確認した上でコンテンツ鍵Ｋｃが再生回路１５０へ送信され、不正なコンテンツデータの再生を禁止することができる。

【０２４３】

また、上述したように、ハードディスクにおいて相当数記憶されるライセンスをＬＢＡにより管理することによって、再生許諾セッションにおいて、再生リクエストのあったコンテンツデータに対応するライセンスを、相当数のデータの中から検索することなくダイレクトに取得することができ、迅速な処理が実現できる。

【０２４４】

なお、フローチャートにおいて図示しないが、再生回路１５０は、コンテンツの再生許諾がなされ、コンテンツ鍵Ｋｃを受理すると、ＨＤ２０から出力された暗号化コンテンツデータＥ（Ｋｃ，Ｄｃ）を復号処理部１５１４において復号し、再生部１５１６において復号処理部により復号されたデータＤｃが再生され、ＤＡ変換部１５１８によりデジタル／アナログ変換されてモニタやスピーカなどが接続される端子１５２０へ再生信号が出力される。

【０２４５】

なお、上述した全ての説明においては、コンテンツデータに対するライセンスについて説明したが、対象は、上述したライセンスに限られるものではなく、秘密にする必要がある機密データ一般に拡大されうる。上述した手段によって、データの機密性が保護され、かつ、データ記憶装置における機密データの特定に関する本発明の目的が達成できるからである。

【０２４６】

今回開示された実施の形態は、すべての点で例示であって制限的なものではないと考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

【図面の簡単な説明】

【図１】　データ配信システムを概念的に説明する概略図である。

【図２】　図１に示すデータ配信システムにおいて送受信されるデータ、情報等の特性を示す図である。

【図３】　図１に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を示す図である。

【図４】　図１に示すライセンス提供装置の構成を示す概略ブロック図である。

【図５】　図１に示す端末装置の構成を示す概略ブロック図である。

【図６】　図１に示す端末装置に装着されるハードディスクの構成を示す概略ブロック図である。

【図７】　図６に示すハードディスクにおけるセキュアデータ記憶部のメモリ構成を示す図である。

【図８】　図１に示すデータ配信システムにおける配信処理を説明するための第１のフローチャートである。

【図９】　図１に示すデータ配信システムにおける配信処理を説明するための第２のフローチャートである。

【図１０】　図１に示すデータ配信システムにおける配信処理中の再書込処理を説明するための第１のフローチャートである。

【図１１】　図１に示すデータ配信システムにおける配信処理中の再書込処理を説明するための第２のフローチャートである。

【図１２】　図１に示すデータ配信システムにおける配信処理中の再書込処理を説明するための第３のフローチャートである。

【図１３】　複製・移動処理が行なわれるシステム構成を概念的に説明する概略図である。

【図１４】　図１３に示すシステムにおける複製または移動処理を説明するための第１のフローチャートである。

【図１５】　図１３に示すシステムにおける複製または移動処理を説明するための第２のフローチャートである。

【図１６】　図１３に示すシステムにおける複製または移動処理中の再書込

処理を説明するための第１のフローチャートである。

【図１７】　図１３に示すシステムにおける複製または移動処理中の再書込処理を説明するための第２のフローチャートである。

【図１８】　図１３に示すシステムにおける複製または移動処理中の再書込処理を説明するための第３のフローチャートである。

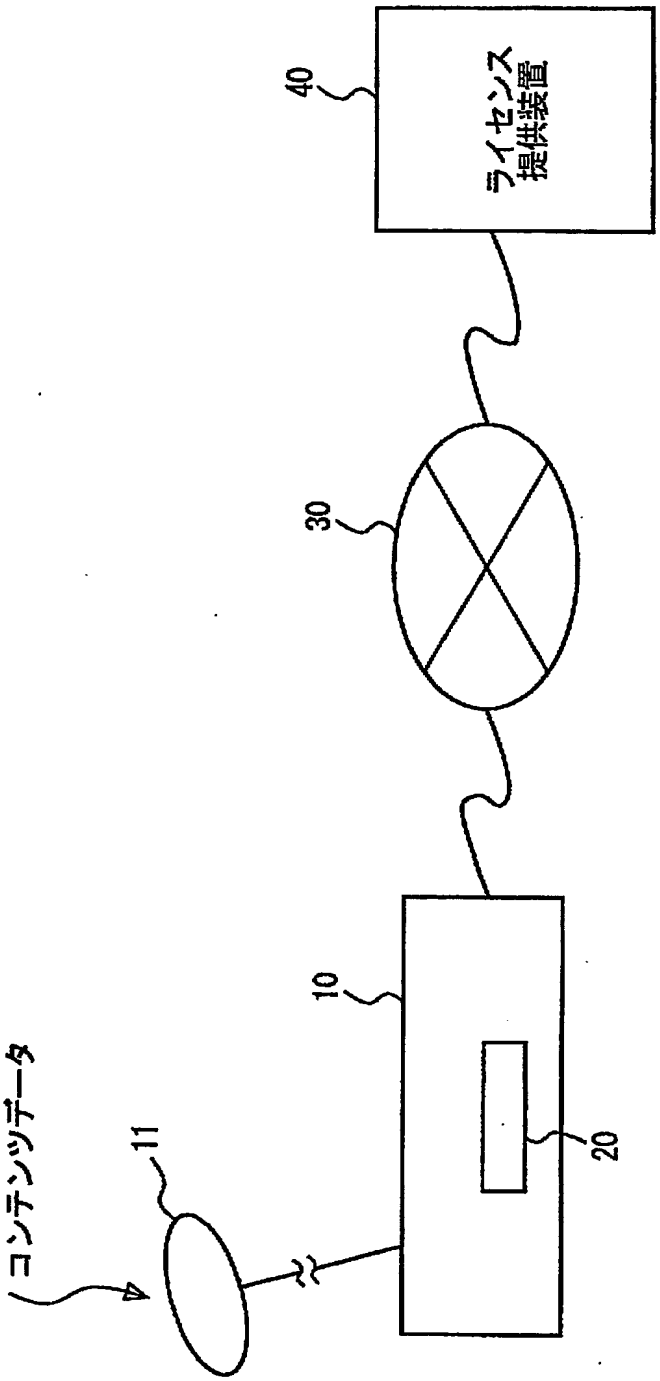
【図１９】　図５に示す端末装置に対する再生許諾処理を説明するためのフローチャートである。

【符号の説明】

１０　端末装置、１１　アンテナ、２０，２１　ハードディスク、３０　ネットワーク、４０　ライセンス提供装置、１０２　アンテナ、１０４　受信部、１０６　モデム、１０８　コントローラ、１１０　ＨＤインターフェース部、１５０　再生回路、２０２，１５０２　認証データ保持部、２０４　Ｋｃｍ保持部、２０６　Ｋｏｍ保持部、２０８　ＫＰｏｍ保持部、２１０，１５２０　端子、２１２　ＡＴＡインターフェース部、２１４　コントローラ、２１６，２２８，２３０，４２２，１５０６，１５１２，１５１４　復号処理部、２１８，４１６　ＫＰａ保持部、２２０，４１８　認証部、２２２，２２４，２３２，４２０，４２４，４２６，１５１０　暗号処理部、２２６，４１４，１５０８　セッション鍵発生部、２５０　セキュアデータ記憶部、２５０Ａ　セキュアデータメモリ、２５０Ｂ　ログメモリ、２５０Ｃ　有効フラグメモリ、２６０，２６２　切替スイッチ、２７０　ノーマルデータ記憶部、４０２　コンテンツＤＢ、４０４　ログＤＢ、４１０　データ処理部、４１２　配信制御部、４５０　通信装置、１５０４　Ｋｃｐ保持部、１５１６　再生部、１５１８　ＤＡ変換部、２５０１　ライセンスＩＤ領域、２５０２　Ｋｓ２ｘ領域、２５０３　ＳＴ１領域，２５０４　ＳＴ２領域、２５０５　ＫＰｃｍｘ領域、２５０６　ＬＢＡ領域、２７０１　磁気記録媒体、２７０２　モータ、２７０３　サーボ制御部、２７０４　シーク制御部、２７０５　記録再生処理部、ＢＳ１～ＢＳ３　バス。

【書類名】　図面

【図１】



【図２】

記号	名称	属性	特性
Dc	データ	データ固有	例：映像データ、音楽データ、朗読データ、教材データ、画像データ、ゲームプログラム Kcにて暗号化した暗号化コンテンツデータ E(Kc, Dc)として記録管理される
Di	データ情報	データ固有	Dcに付随する平文データ。DIDを含む
DID	データID	データ固有	DcおよびKcを特定するための管理コード
Kc	コンテンツ鍵	データ固有	暗号データを暗号／復号する共通鍵
AC	制御情報	ライセンス固有	再生やライセンスの取扱いに関する制限事項
LID	ライセンスID	ライセンス固有	ライセンスを特定するための管理コード
LIC	ライセンス	ライセンス固有	Kc//AC//DID//LIDの総称

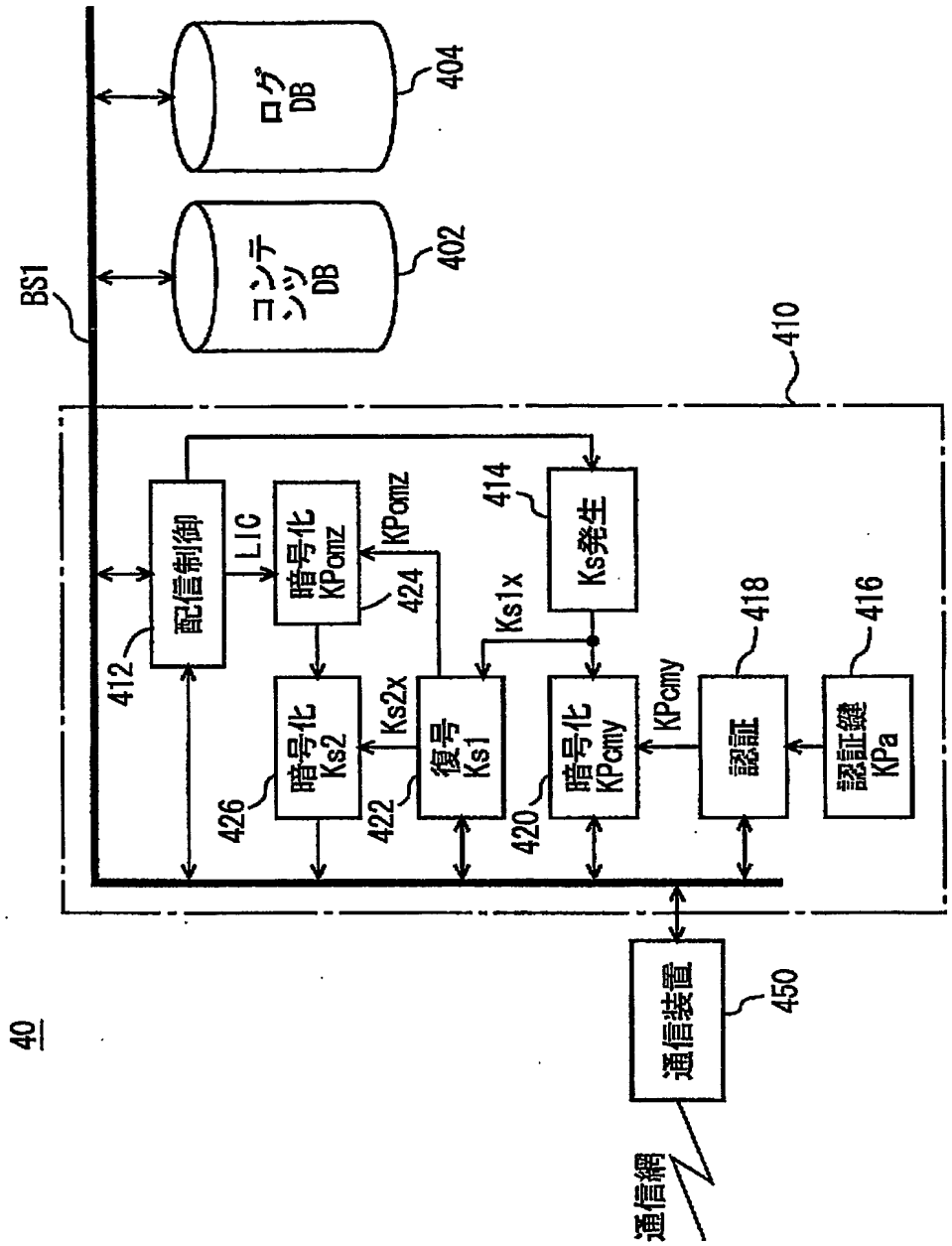
【図３】

	記号	名称	特性
ライセンス提供装置	KPa	認証鍵	認証局にて証明書を検証する公開復号鍵 ライセンス提供側にて運用される
	Ks1x	セッション鍵	ライセンスの配信ごとに生成される一時鍵 共通鍵
データ記録装置 (ハードディスク)	Ka	マスタ鍵	クラス証明書作成のために使用する秘密暗号鍵 認証局にて運用される
	KPa	認証鍵	認証局にて証明書を検証する公開復号鍵 ライセンス提供側にて運用される
	KPcmy	クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 「y」はクラスを識別するための識別子
	Kcmy	クラス秘密鍵	クラス公開鍵KPcmyにて暗号化されたデータを復号する非対称な復号鍵
	Icmy	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	Cmy	クラス証明書	Cmy=KPcmy//Icmy//E(Ka,H(KPcmy//Icmy)) 認証鍵KPaによってその正当性が確認できる
	KPcmz	個別公開鍵	データ記録装置ごとに固有な値を持つ個別公開暗号鍵 「z」はデータ記録装置を識別するための識別子
	Kcmz	個別秘密鍵	個別公開鍵KPcmzにて暗号化されたデータを復号する非対称な復号鍵
	Ks1x	セッション鍵	ライセンスの授受ごとにライセンス提供側で生成される一時鍵 共通鍵
	Ks2x	セッション鍵	ライセンスの授受ごとにライセンス受理側で生成される一時鍵 共通鍵
再生回路	KPcpy	クラス公開鍵	機器のクラス(種類などの一定の単位ごと)に付与される暗号鍵 「y」はクラスを識別するための識別子
	Kcpy	クラス秘密鍵	クラス公開鍵KPcpyにて暗号化されたデータを復号する非対称な復号鍵
	Icpy	クラス情報	クラスごとの機器およびクラス公開鍵に関する情報データ
	Cpy	クラス証明書	Cpy=KPcpy//Icpy//E(Ka,H(KPcpy//Icpy)) 認証鍵KPaによってその正当性が確認できる
	Ks2x	セッション鍵	ライセンスの授受ごとにライセンス受理側で生成される一時鍵 共通鍵

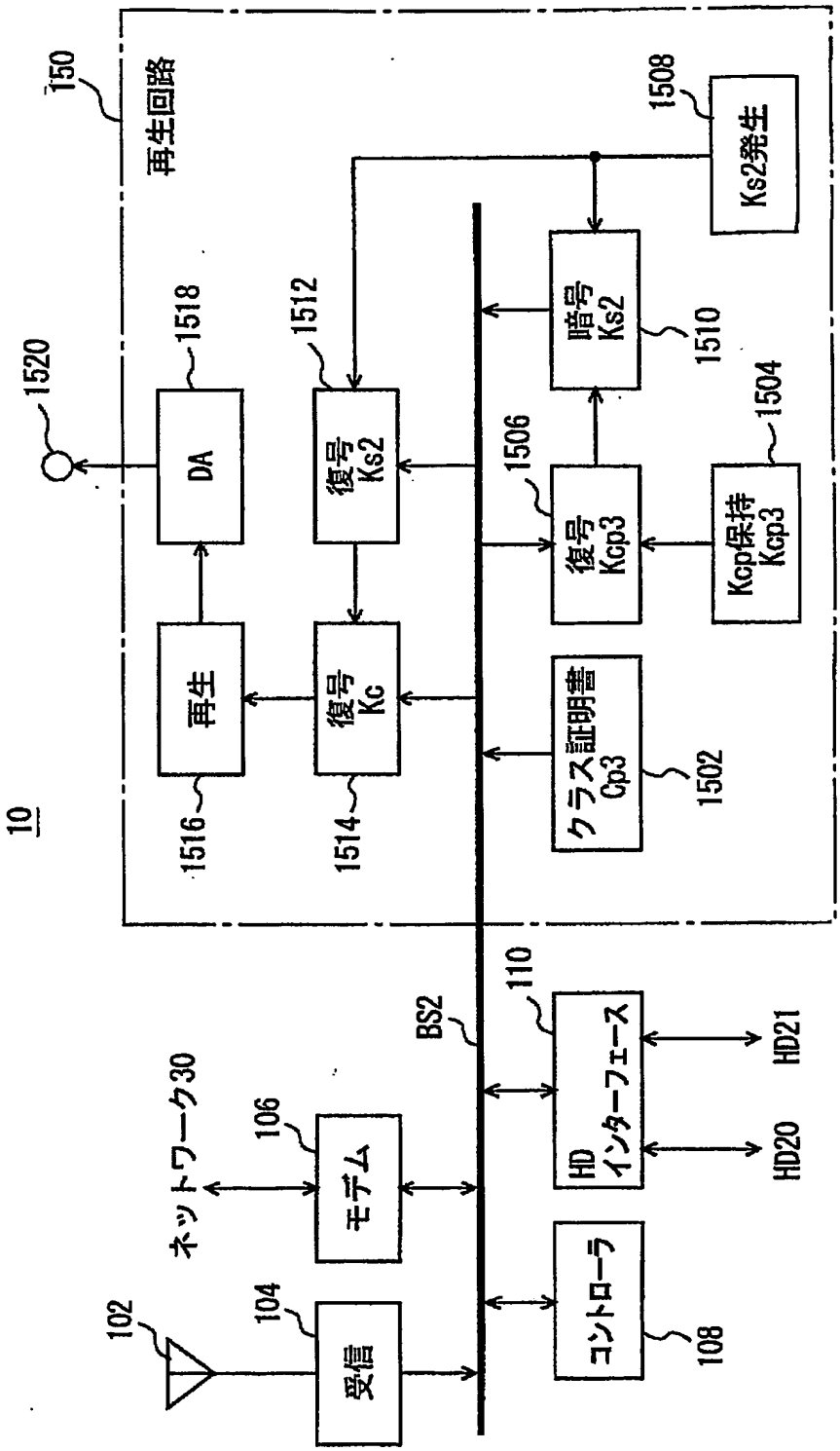
出証特２００３－３０２４２７９

特２００２－０５９１７９

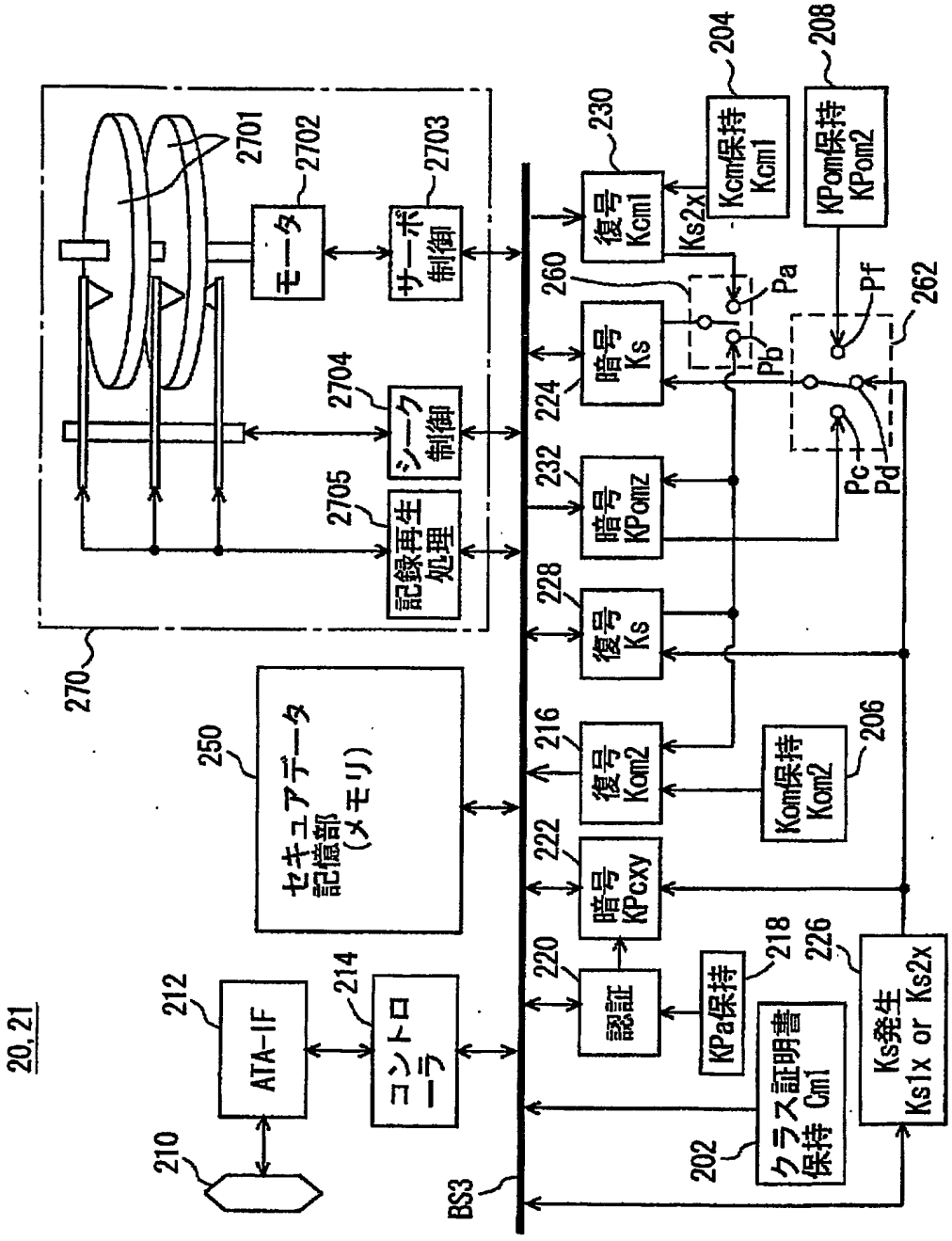
【図４】


40
BS1
ログDB
404
コンテンツDB
402
410
配信制御
412
LIC
暗号化 KPcmz
424
KPcmz
414
Ks発生
Ks1x
暗号化 Ks2
426
Ks2x
復号 Ks1
422
暗号化 KPcmy
420
KPcmy
認証
418
認証鍵 KPa
416
通信装置
450
通信網

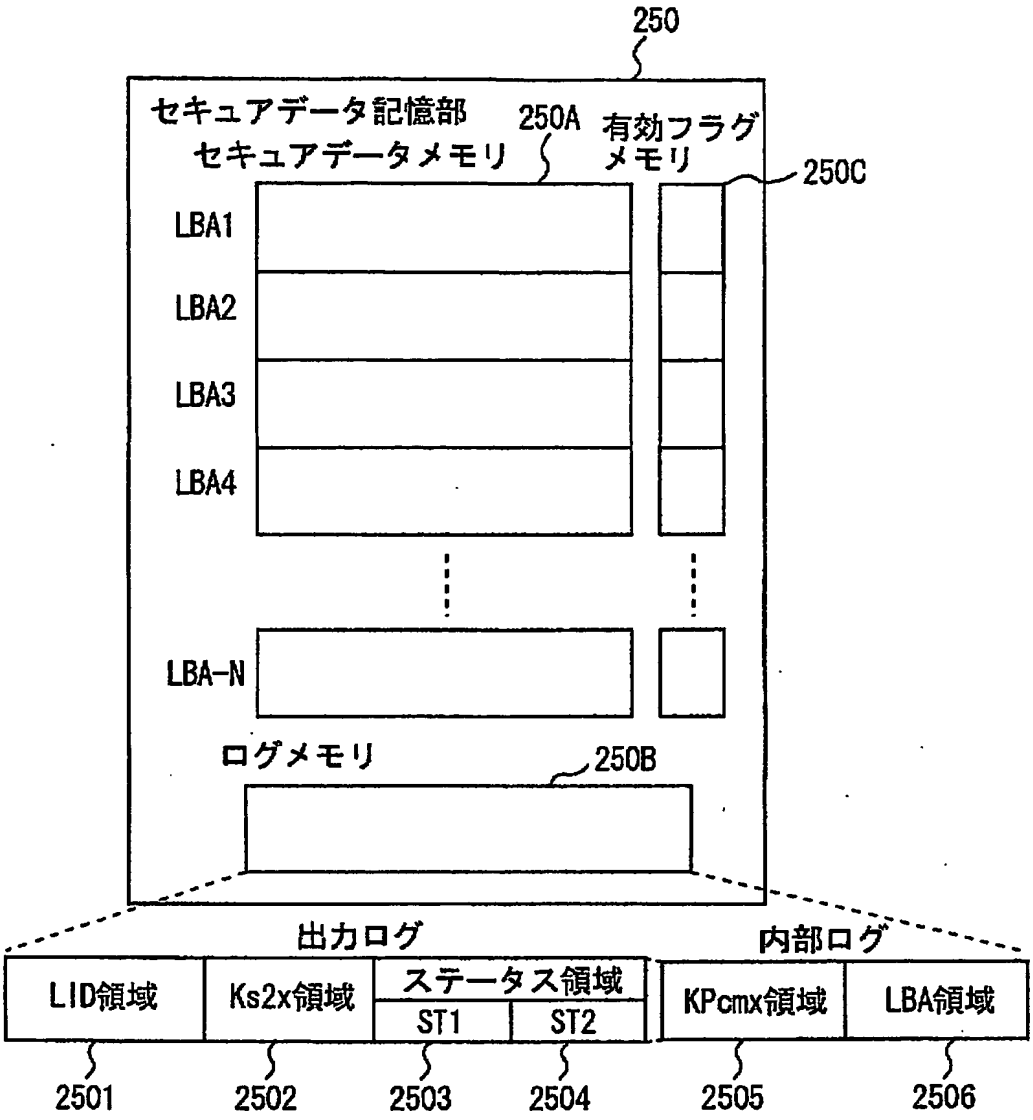
【図５】


10
150
再生回路
1508
Ks2発生
暗号 Ks2
1510
1512
復号 Ks2
1518
DA
1520
1504
Kcp保持 Kcp3
1506
復号 Kcp3
クラス証明書 Cp3
1502
1514
復号 Kc
1516
再生
BS2
110
HD インターフェース
HD21
HD20
ネットワーク30
106
モデム
102
104
受信
コントローラ
108

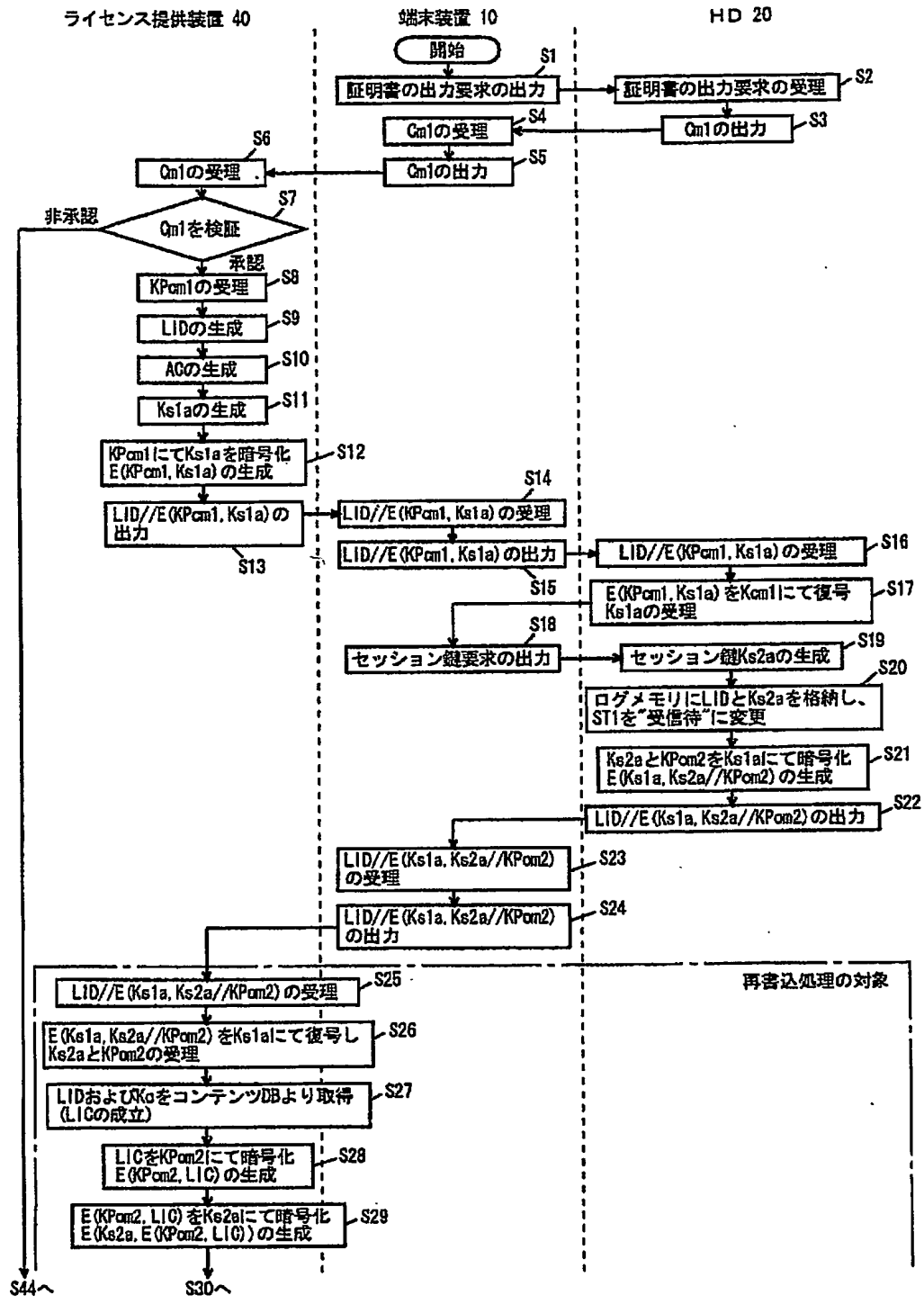
【図６】


20,21
ATA-IF
212
210
コントローラ
214
セキュアデータ記憶部（メモリ）
250
270
2701
2702
モータ
2703
サーボ制御
2704
シーク制御
2705
記録再生処理
BS3
220
認証
222
暗号 KPcxy
216
復号 Kcm2
228
復号 Ks
232
暗号 KPcm2
224
暗号 Ks
230
復号 Kcm1
260
Ks2x
204
Kcm保持 Kcm1
208
KPcm保持 KPcm2
Pa
Pb
Pc
Pd
Pf
262
206
Kcm保持 Kcm2
218
KPa保持
226
Ks発生 Ks1x or Ks2x
202
クラス証明書保持 Cm1

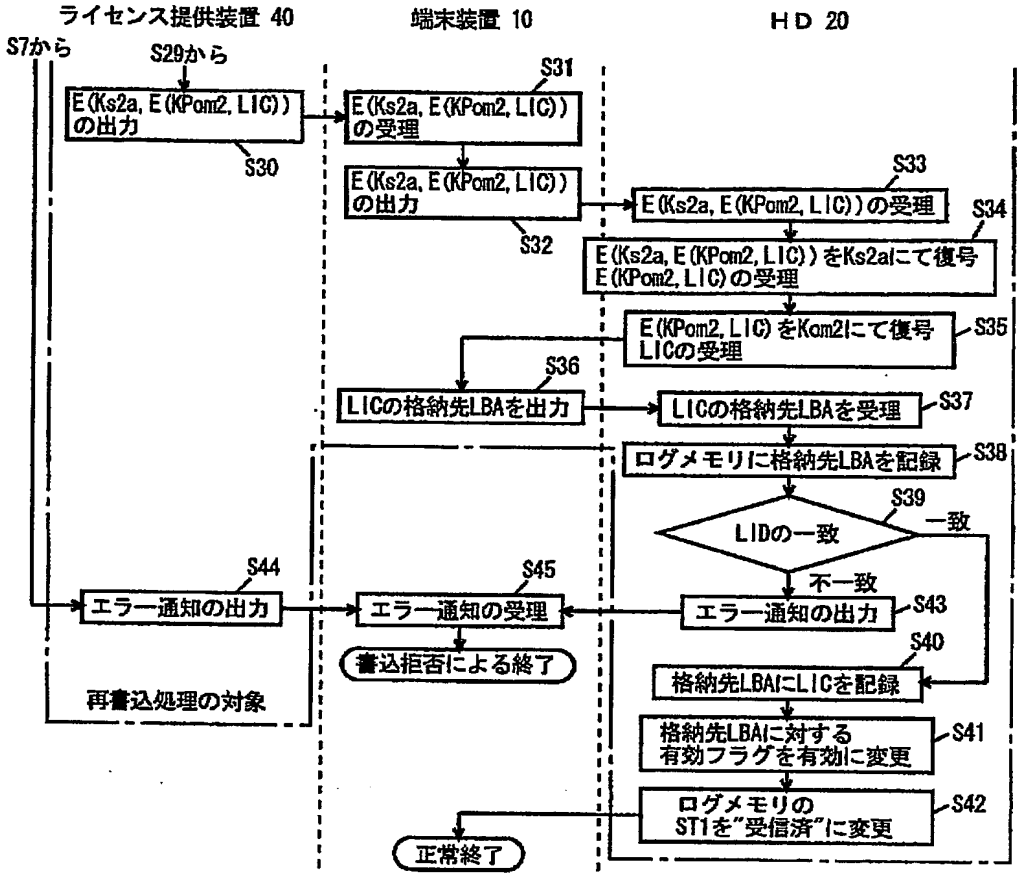
【図７】


250
セキュアデータ記憶部
セキュアデータメモリ
250A
有効フラグ
メモリ
250C
LBA1
LBA2
LBA3
LBA4
LBA-N
ログメモリ
250B
出力ログ
内部ログ
LID領域
Ks2x領域
ステータス領域
ST1
ST2
KPcmx領域
LBA領域
2501
2502
2503
2504
2505
2506

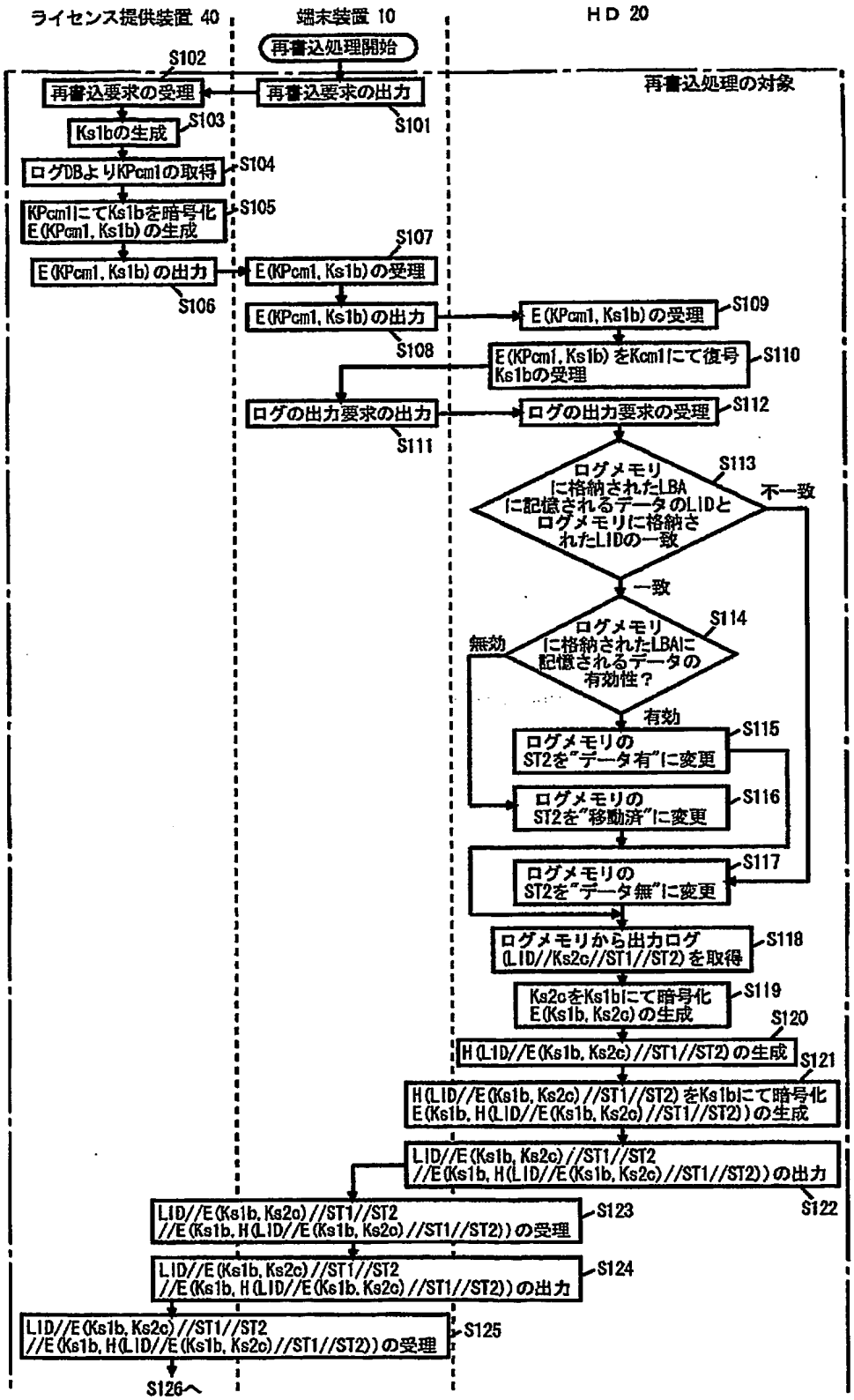
【図８】


ライセンス提供装置 40
端末装置 10
HD 20
開始
S1
証明書の出力要求の出力
S2
証明書の出力要求の受理
S3
Cm1の出力
S4
Cm1の受理
S5
Cm1の出力
S6
Cm1の受理
S7
Cm1を検証
非承認
承認
S8
KPcm1の受理
S9
LIDの生成
S10
ACの生成
S11
Ks1aの生成
S12
KPcm1にてKs1aを暗号化
E(KPcm1, Ks1a)の生成
S13
LID//E(KPcm1, Ks1a)の出力
S14
LID//E(KPcm1, Ks1a)の受理
LID//E(KPcm1, Ks1a)の出力
S15
S16
LID//E(KPcm1, Ks1a)の受理
S17
E(KPcm1, Ks1a)をKcm1にて復号
Ks1aの受理
S18
セッション鍵要求の出力
S19
セッション鍵Ks2aの生成
S20
ログメモリにLIDとKs2aを格納し、
ST1を"受信待"に変更
S21
Ks2aとKPcm2をKs1aにて暗号化
E(Ks1a, Ks2a//KPcm2)の生成
S22
LID//E(Ks1a, Ks2a//KPcm2)の出力
S23
LID//E(Ks1a, Ks2a//KPcm2)
の受理
S24
LID//E(Ks1a, Ks2a//KPcm2)
の出力
再書込処理の対象
S25
LID//E(Ks1a, Ks2a//KPcm2)の受理
S26
E(Ks1a, Ks2a//KPcm2)をKs1aにて復号し
Ks2aとKPcm2の受理
S27
LIDおよびKcをコンテンツDBより取得
(LICの成立)
S28
LICをKPcm2にて暗号化
E(KPcm2, LIC)の生成
S29
E(KPcm2, LIC)をKs2aにて暗号化
E(Ks2a, E(KPcm2, LIC))の生成
S44へ
S30へ

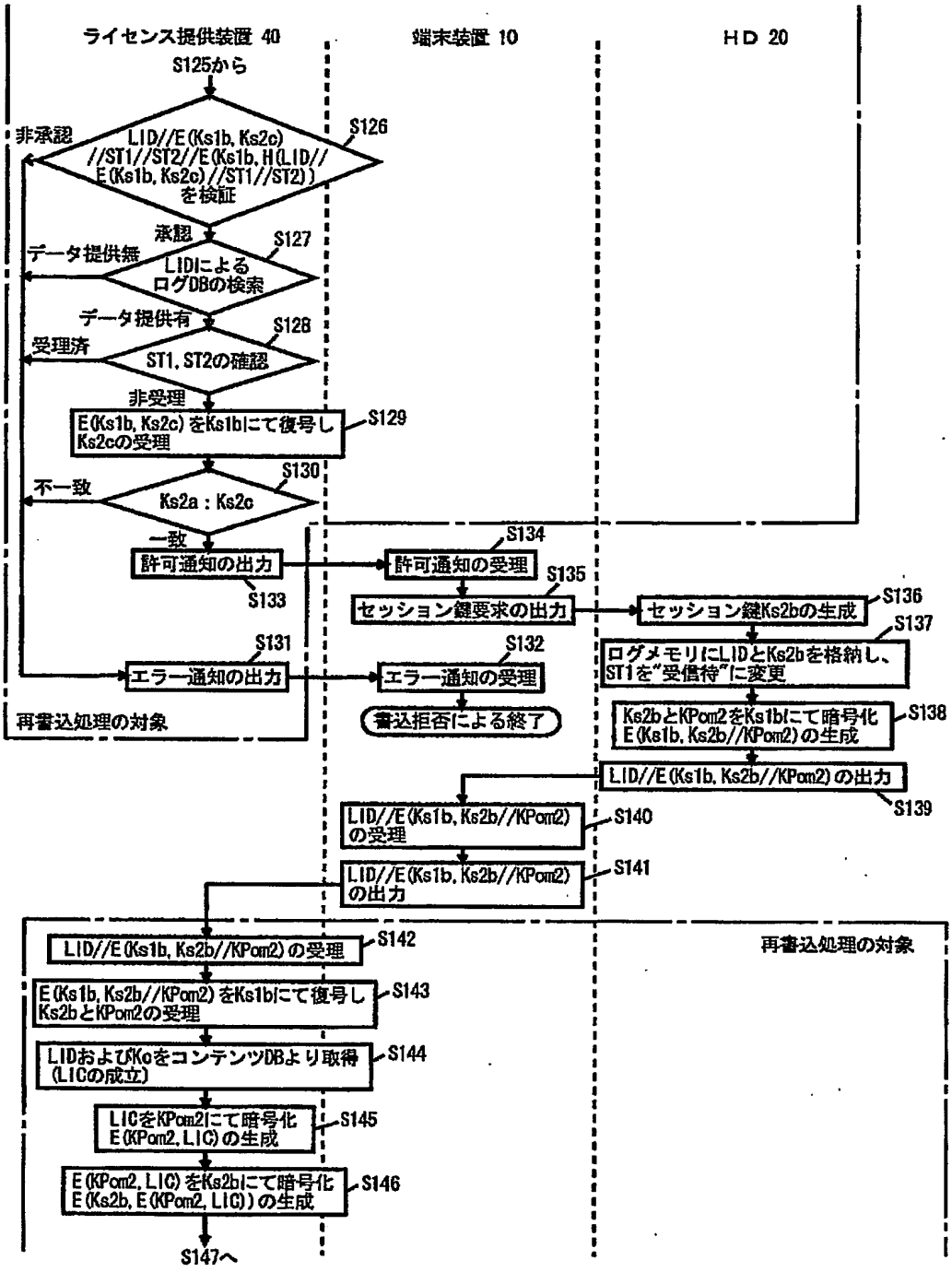
【図９】


ライセンス提供装置 40
端末装置 10
HD 20
S7から
S29から
E(Ks2a, E(KPom2, LIC))の出力
S30
S31
E(Ks2a, E(KPom2, LIC))の受理
E(Ks2a, E(KPom2, LIC))の出力
S32
S33
E(Ks2a, E(KPom2, LIC))の受理
S34
E(Ks2a, E(KPom2, LIC))をKs2aにて復号 E(KPom2, LIC)の受理
E(KPom2, LIC)をKom2にて復号 LICの受理
S35
S36
LICの格納先LBAを出力
LICの格納先LBAを受理
S37
ログメモリに格納先LBAを記録
S38
S39
LIDの一致
一致
不一致
S44
S45
エラー通知の出力
エラー通知の受理
エラー通知の出力
S43
書込拒否による終了
S40
格納先LBAにLICを記録
格納先LBAに対する有効フラグを有効に変更
S41
ログメモリのST1を"受信済"に変更
S42
正常終了
再書込処理の対象

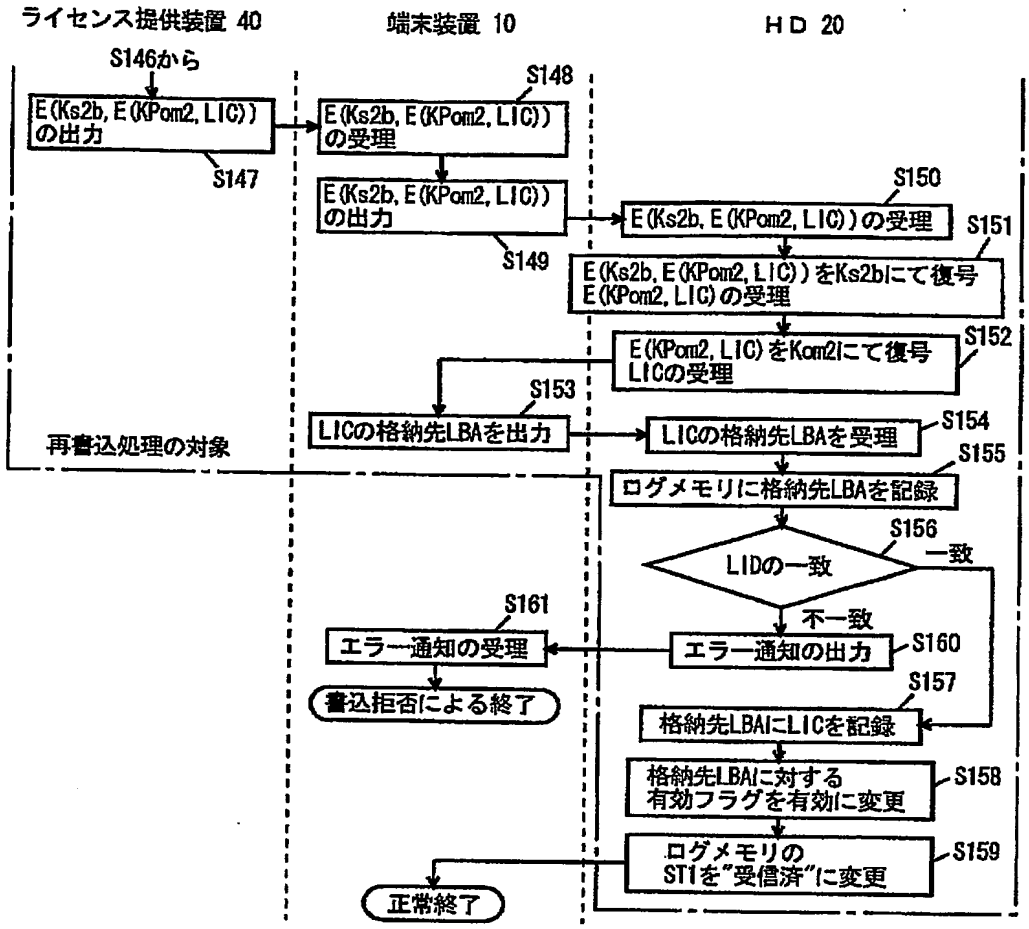
【図１０】


ライセンス提供装置 40
端末装置 10
HD 20
再書込処理開始
S102
再書込要求の受理
再書込要求の出力
S101
再書込処理の対象
Ks1bの生成
S103
ログDBよりKPcm1の取得
S104
KPcm1にてKs1bを暗号化
E(KPcm1, Ks1b)の生成
S105
S107
E(KPcm1, Ks1b)の出力
E(KPcm1, Ks1b)の受理
S106
E(KPcm1, Ks1b)の出力
E(KPcm1, Ks1b)の受理
S109
S108
E(KPcm1, Ks1b)をKcm1にて復号
Ks1bの受理
S110
ログの出力要求の出力
ログの出力要求の受理
S112
S111
ログメモリ
に格納されたLBA
に記憶されるデータのLIDと
ログメモリに格納さ
れたLIDの一致
S113
不一致
一致
ログメモリ
に格納されたLBAに
記憶されるデータの
有効性？
S114
無効
有効
ログメモリの
ST2を"データ有"に変更
S115
ログメモリの
ST2を"移動済"に変更
S116
ログメモリの
ST2を"データ無"に変更
S117
ログメモリから出力ログ
(LID//Ks2c//ST1//ST2)を取得
S118
Ks2cをKs1bにて暗号化
E(Ks1b, Ks2c)の生成
S119
S120
H(LID//E(Ks1b, Ks2c)//ST1//ST2)の生成
S121
H(LID//E(Ks1b, Ks2c)//ST1//ST2)をKs1bにて暗号化
E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の生成
LID//E(Ks1b, Ks2c)//ST1//ST2
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の出力
S122
LID//E(Ks1b, Ks2c)//ST1//ST2
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の受理
S123
LID//E(Ks1b, Ks2c)//ST1//ST2
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の出力
S124
LID//E(Ks1b, Ks2c)//ST1//ST2
//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の受理
S125
S126へ

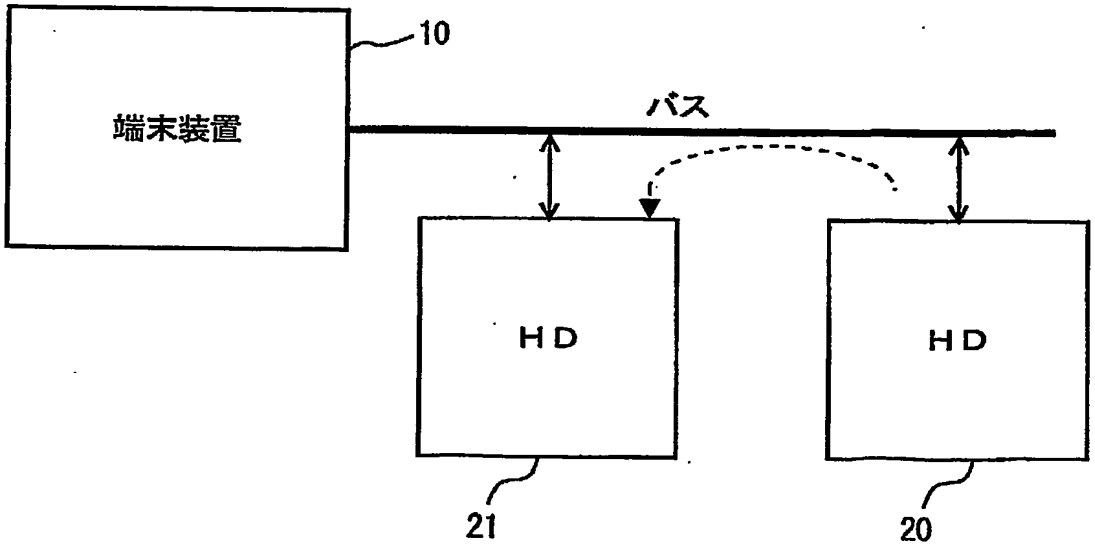
【図１１】


ライセンス提供装置 40
端末装置 10
HD 20
S125から
S126
LID//E(Ks1b, Ks2c)//ST1//ST2//E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))を検証
非承認
承認
S127
LIDによるログDBの検索
データ提供無
データ提供有
S128
ST1, ST2の確認
受理済
非受理
S129
E(Ks1b, Ks2c)をKs1bにて復号しKs2cの受理
S130
Ks2a：Ks2c
不一致
一致
許可通知の出力
S133
S134
許可通知の受理
S135
セッション鍵要求の出力
S136
セッション鍵Ks2bの生成
S137
ログメモリにLIDとKs2bを格納し、ST1を"受信待"に変更
S131
エラー通知の出力
S132
エラー通知の受理
書込拒否による終了
再書込処理の対象
S138
Ks2bとKPom2をKs1bにて暗号化E(Ks1b, Ks2b//KPom2)の生成
LID//E(Ks1b, Ks2b//KPom2)の出力
S139
LID//E(Ks1b, Ks2b//KPom2)の受理
S140
LID//E(Ks1b, Ks2b//KPom2)の出力
S141
再書込処理の対象
LID//E(Ks1b, Ks2b//KPom2)の受理
S142
E(Ks1b, Ks2b//KPom2)をKs1bにて復号しKs2bとKPom2の受理
S143
LIDおよびKoをコンテンツDBより取得(LICの成立)
S144
LICをKPom2にて暗号化E(KPom2, LIC)の生成
S145
E(KPom2, LIC)をKs2bにて暗号化E(Ks2b, E(KPom2, LIC))の生成
S146
S147へ

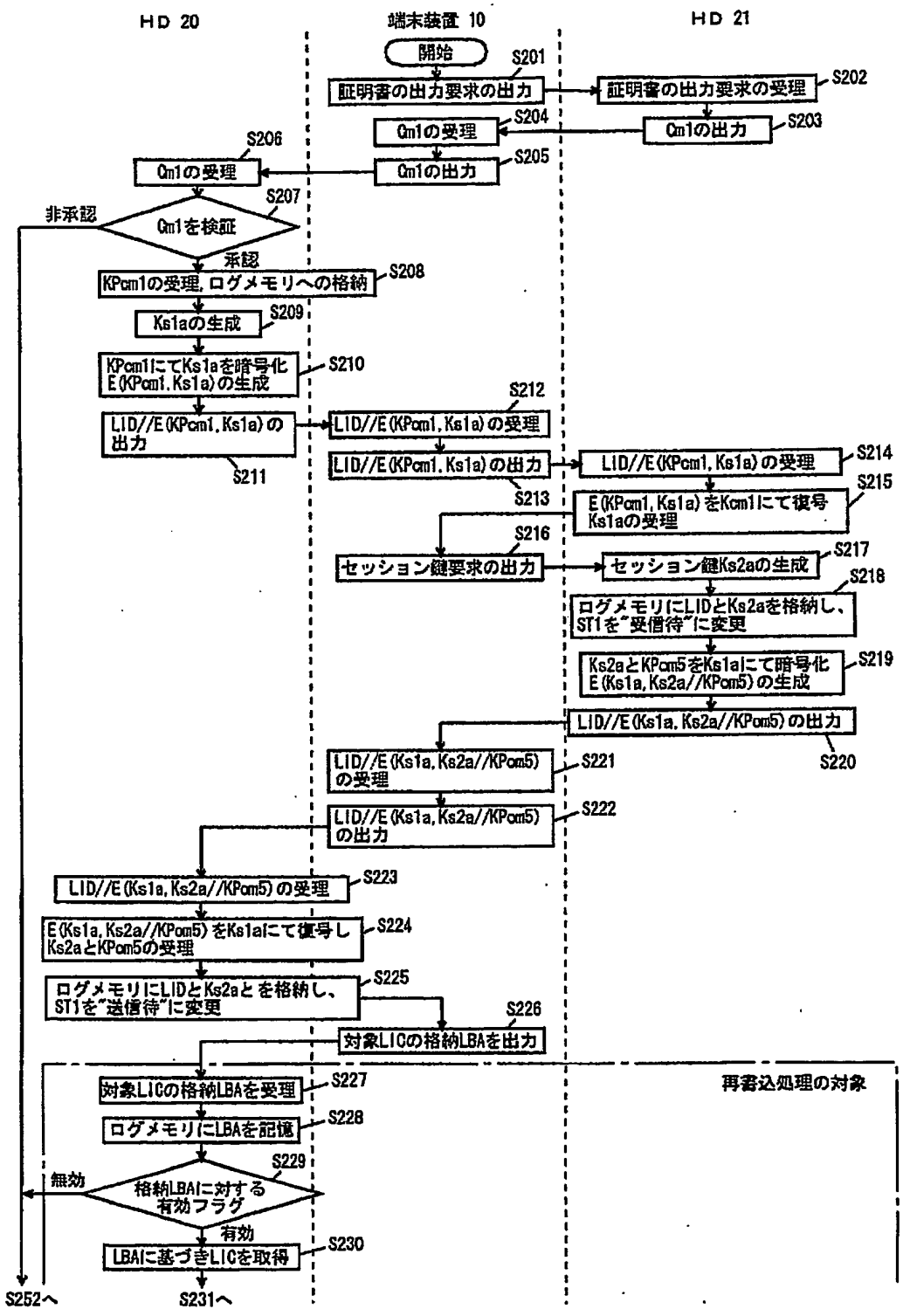
【図１２】


ライセンス提供装置 40
端末装置 10
HD 20
S146から
E(Ks2b, E(KPom2, LIC))の出力
S147
S148
E(Ks2b, E(KPom2, LIC))の受理
E(Ks2b, E(KPom2, LIC))の出力
S149
S150
E(Ks2b, E(KPom2, LIC))の受理
S151
E(Ks2b, E(KPom2, LIC))をKs2bにて復号
E(KPom2, LIC)の受理
E(KPom2, LIC)をKom2にて復号
LICの受理
S152
S153
LICの格納先LBAを出力
LICの格納先LBAを受理
S154
再書込処理の対象
S155
ログメモリに格納先LBAを記録
S156
LIDの一致
一致
不一致
S161
エラー通知の受理
エラー通知の出力
S160
書込拒否による終了
S157
格納先LBAにLICを記録
格納先LBAに対する
有効フラグを有効に変更
S158
ログメモリの
ST1を"受信済"に変更
S159
正常終了

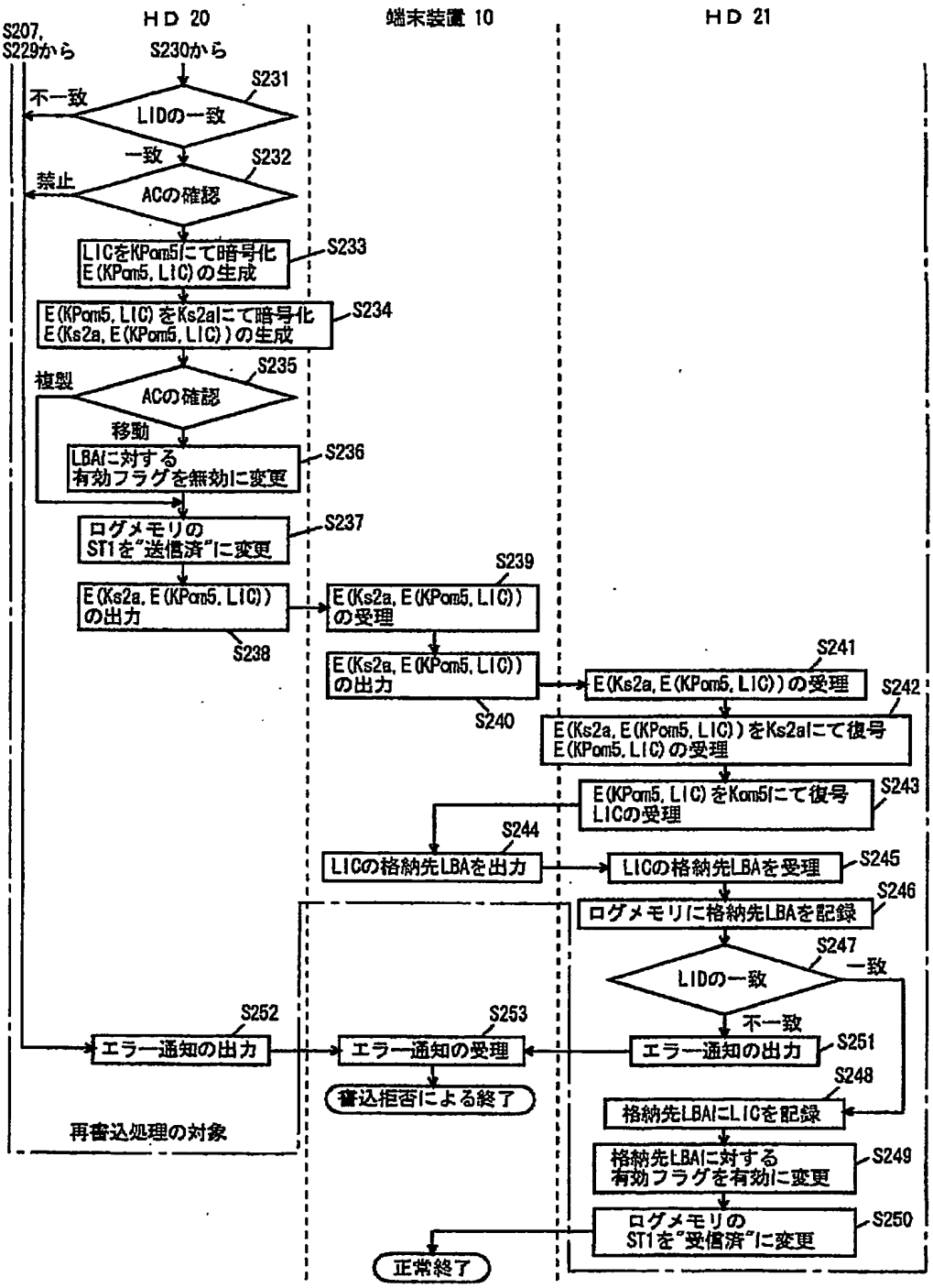
【図１３】


10
端末装置
バス
HD
HD
21
20

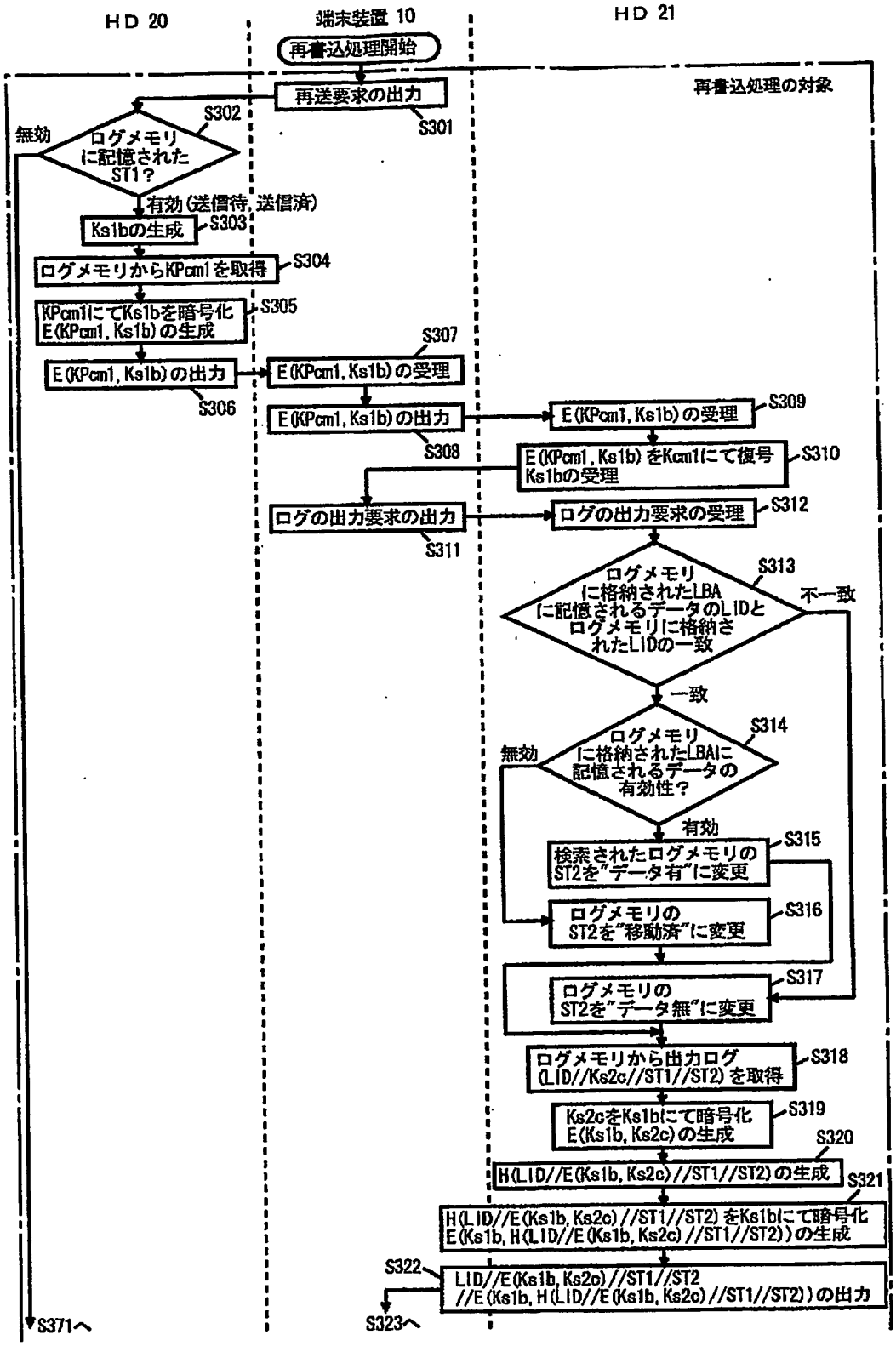
【図１４】


HD 20
端末装置 10
HD 21
開始
S201
証明書の出力要求の出力
証明書の出力要求の受理
S202
Cm1の受理
S204
Cm1の出力
S203
S206
Cm1の受理
Cm1の出力
S205
S207
非承認
Cm1を検証
承認
KPcm1の受理, ログメモリへの格納
S208
Ks1aの生成
S209
KPcm1にてKs1aを暗号化
E(KPcm1, Ks1a)の生成
S210
S212
LID//E(KPcm1, Ks1a)の出力
LID//E(KPcm1, Ks1a)の受理
S211
LID//E(KPcm1, Ks1a)の出力
LID//E(KPcm1, Ks1a)の受理
S214
S213
E(KPcm1, Ks1a)をKcm1にて復号
Ks1aの受理
S215
S216
セッション鍵要求の出力
セッション鍵Ks2aの生成
S217
S218
ログメモリにLIDとKs2aを格納し、
ST1を"受信待"に変更
Ks2aとKPcm5をKs1aにて暗号化
E(Ks1a, Ks2a//KPcm5)の生成
S219
LID//E(Ks1a, Ks2a//KPcm5)の出力
S220
LID//E(Ks1a, Ks2a//KPcm5)
の受理
S221
LID//E(Ks1a, Ks2a//KPcm5)
の出力
S222
LID//E(Ks1a, Ks2a//KPcm5)の受理
S223
E(Ks1a, Ks2a//KPcm5)をKs1aにて復号し
Ks2aとKPcm5の受理
S224
ログメモリにLIDとKs2aとを格納し、
ST1を"送信待"に変更
S225
S226
対象LICの格納LBAを出力
再書込処理の対象
対象LICの格納LBAを受理
S227
ログメモリにLBAを記憶
S228
S229
無効
格納LBAに対する
有効フラグ
有効
LBAに基づきLICを取得
S230
S252へ
S231へ

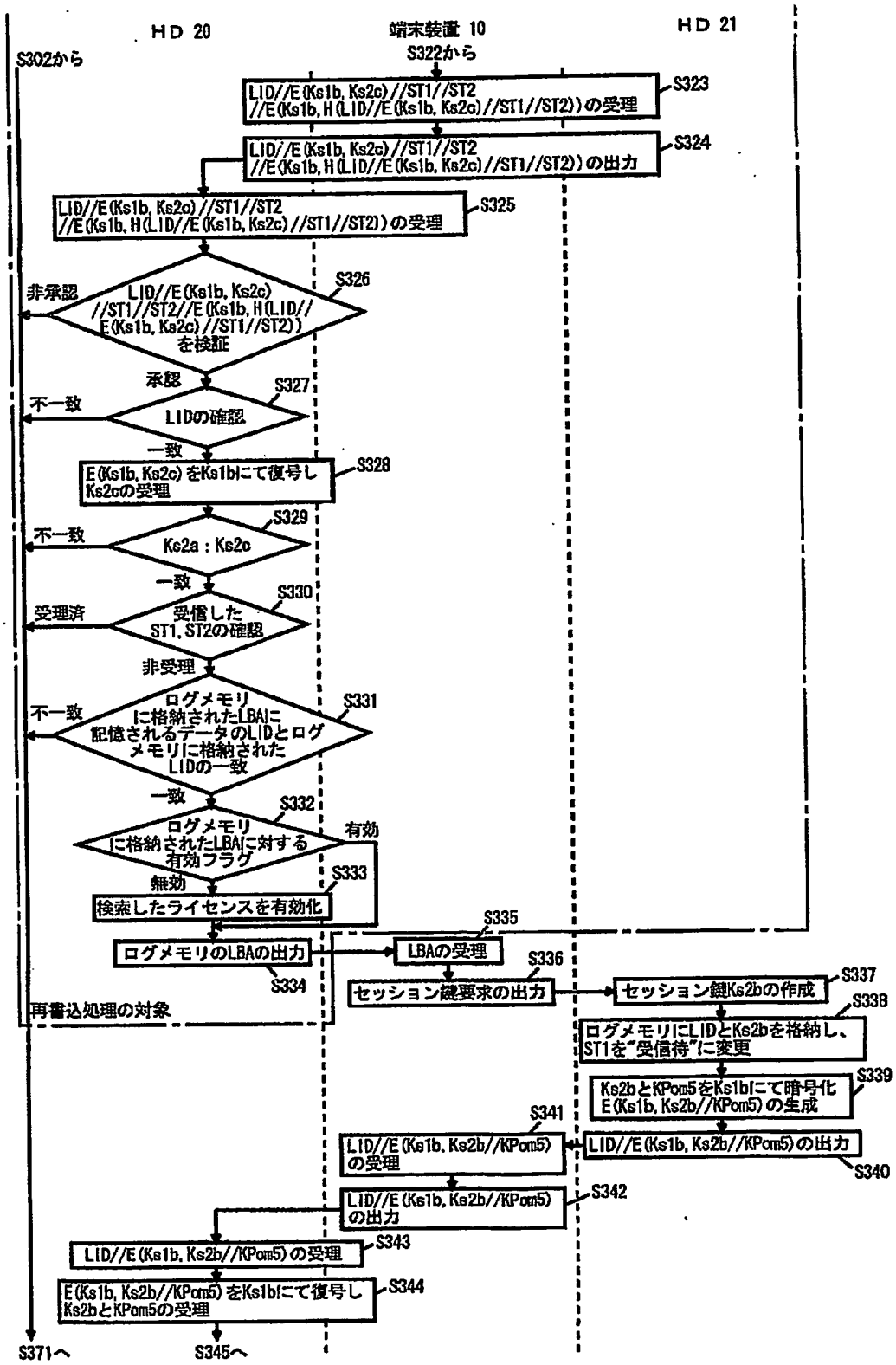
【図１５】


HD 20
端末装置 10
HD 21
S207,
S229から
S230から
S231
不一致
LIDの一致
一致
S232
禁止
ACの確認
LICをKPam5にて暗号化
E(KPam5, LIC)の生成
S233
E(KPam5, LIC)をKs2aにて暗号化
E(Ks2a, E(KPam5, LIC))の生成
S234
S235
複製
ACの確認
移動
LBAに対する
有効フラグを無効に変更
S236
ログメモリの
ST1を"送信済"に変更
S237
E(Ks2a, E(KPam5, LIC))
の出力
S238
S239
E(Ks2a, E(KPam5, LIC))
の受理
E(Ks2a, E(KPam5, LIC))
の出力
S240
S241
E(Ks2a, E(KPam5, LIC))の受理
S242
E(Ks2a, E(KPam5, LIC))をKs2aにて復号
E(KPam5, LIC)の受理
E(KPam5, LIC)をKam5にて復号
LICの受理
S243
S244
LICの格納先LBAを出力
LICの格納先LBAを受理
S245
ログメモリに格納先LBAを記録
S246
S247
LIDの一致
一致
不一致
S252
S253
エラー通知の出力
エラー通知の受理
エラー通知の出力
S251
S248
審込拒否による終了
格納先LBAにLICを記録
再審込処理の対象
格納先LBAに対する
有効フラグを有効に変更
S249
ログメモリの
ST1を"受信済"に変更
S250
正常終了

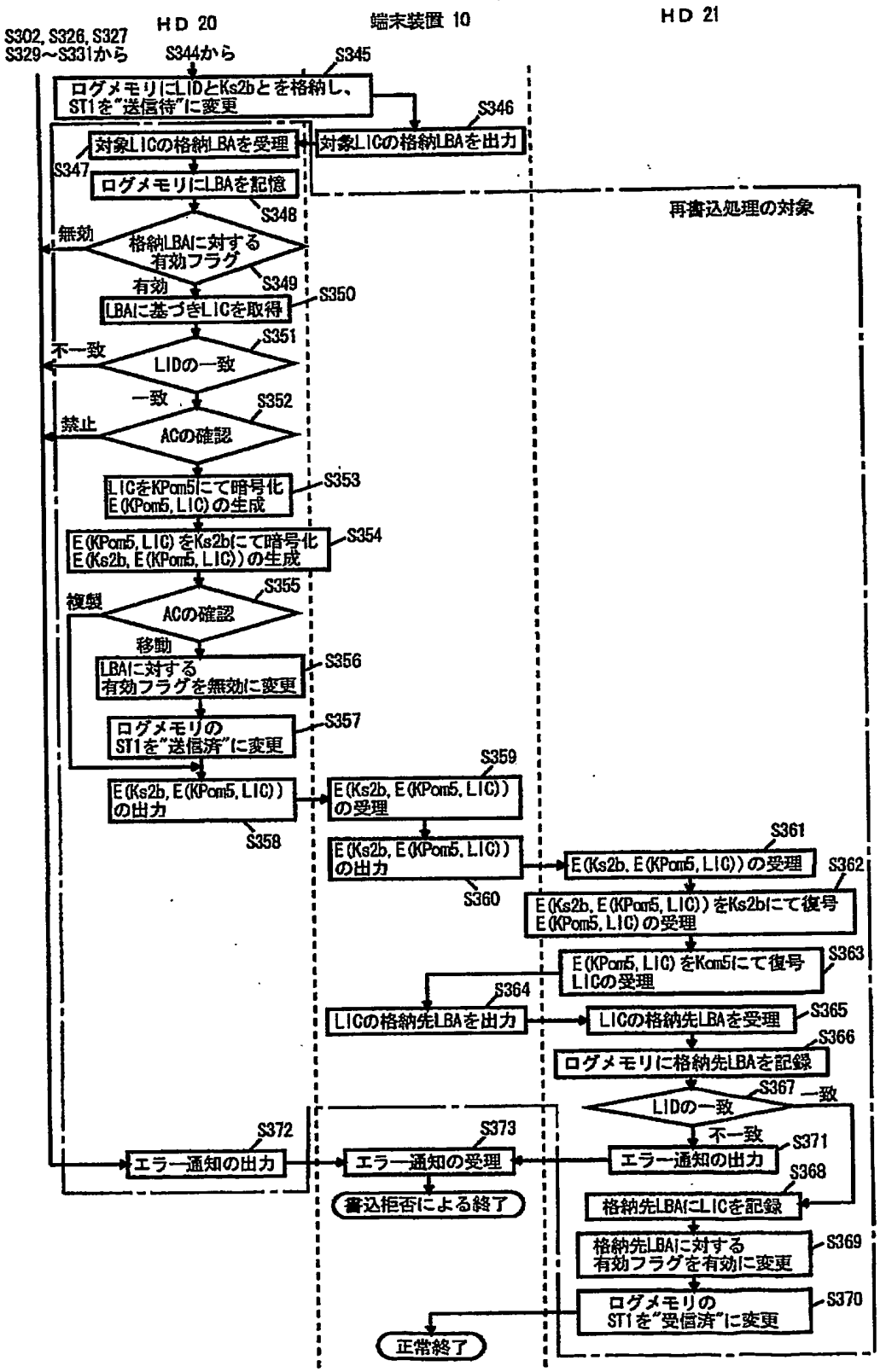
【図１６】


HD 20
端末装置 10
HD 21
再書込処理開始
再書込処理の対象
再送要求の出力
S301
S302
ログメモリに記憶されたST1？
無効
有効(送信待,送信済)
Ks1bの生成
S303
ログメモリからKPcm1を取得
S304
KPcm1にてKs1bを暗号化 E(KPcm1, Ks1b)の生成
S305
E(KPcm1, Ks1b)の出力
S306
S307
E(KPcm1, Ks1b)の受理
E(KPcm1, Ks1b)の出力
S308
E(KPcm1, Ks1b)の受理
S309
E(KPcm1, Ks1b)をKcm1にて復号 Ks1bの受理
S310
ログの出力要求の出力
S311
ログの出力要求の受理
S312
ログメモリに格納されたLBAに記憶されるデータのLIDとログメモリに格納されたLIDの一致
S313
不一致
一致
ログメモリに格納されたLBAに記憶されるデータの有効性？
S314
無効
有効
検索されたログメモリのST2を"データ有"に変更
S315
ログメモリのST2を"移動済"に変更
S316
ログメモリのST2を"データ無"に変更
S317
ログメモリから出力ログ(LID//Ks2c//ST1//ST2)を取得
S318
Ks2cをKs1bにて暗号化 E(Ks1b, Ks2c)の生成
S319
H(LID//E(Ks1b, Ks2c)//ST1//ST2)の生成
S320
H(LID//E(Ks1b, Ks2c)//ST1//ST2)をKs1bにて暗号化 E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の生成
S321
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の出力
S322
S371へ
S323へ

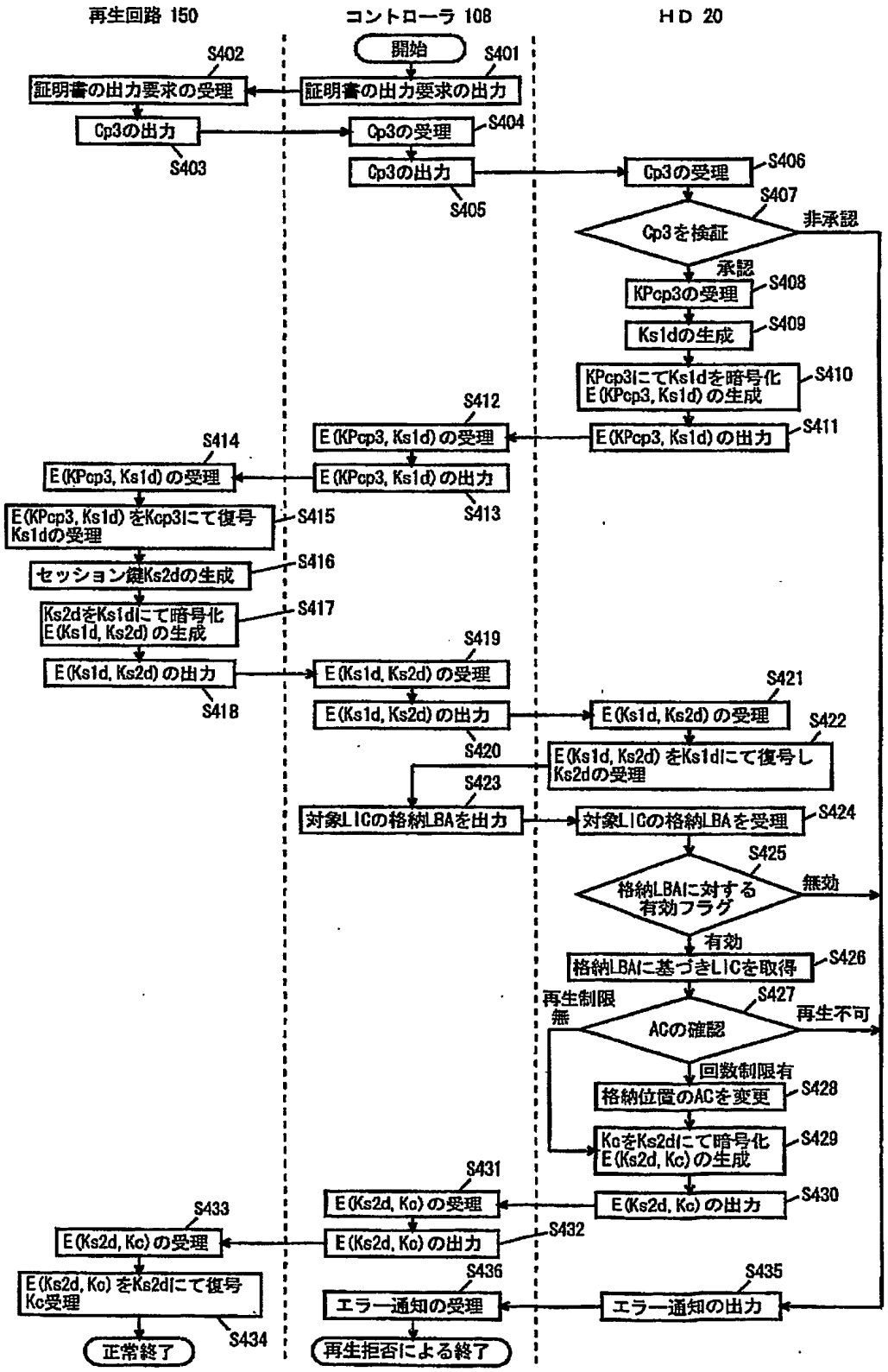
【図１７】


HD 20
端末装置 10
HD 21
S302から
S322から
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の受理
S323
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の出力
S324
LID//E(Ks1b, Ks2c)//ST1//ST2 //E(Ks1b, H(LID//E(Ks1b, Ks2c)//ST1//ST2))の受理
S325
LID//E(Ks1b, Ks2c) //ST1//ST2//E(Ks1b, H(LID// E(Ks1b, Ks2c)//ST1//ST2)) を検証
S326
非承認
承認
LIDの確認
S327
不一致
一致
E(Ks1b, Ks2c)をKs1bにて復号し Ks2cの受理
S328
Ks2a : Ks2c
S329
不一致
一致
受信した ST1, ST2の確認
S330
受理済
非受理
ログメモリ に格納されたLBAに 記憶されるデータのLIDとログ メモリに格納された LIDの一致
S331
不一致
一致
ログメモリ に格納されたLBAに対する 有効フラグ
S332
有効
無効
検索したライセンスを有効化
S333
ログメモリのLBAの出力
S334
LBAの受理
S335
セッション鍵要求の出力
S336
セッション鍵Ks2bの作成
S337
ログメモリにLIDとKs2bを格納し、 ST1を"受信待"に変更
S338
Ks2bとKPom5をKs1bにて暗号化 E(Ks1b, Ks2b//KPom5)の生成
S339
LID//E(Ks1b, Ks2b//KPom5)の出力
S340
LID//E(Ks1b, Ks2b//KPom5) の受理
S341
LID//E(Ks1b, Ks2b//KPom5) の出力
S342
LID//E(Ks1b, Ks2b//KPom5)の受理
S343
E(Ks1b, Ks2b//KPom5)をKs1bにて復号し Ks2bとKPom5の受理
S344
再書込処理の対象
S371へ
S345へ

【図１８】


HD 20
端末装置 10
HD 21
S302, S326, S327
S329～S331から
S344から
S345
ログメモリにLIDとKs2bとを格納し、
ST1を"送信待"に変更
S346
対象LICの格納LBAを出力
対象LICの格納LBAを受理
S347
ログメモリにLBAを記憶
S348
再書込処理の対象
無効
格納LBAに対する
有効フラグ
S349
有効
LBAに基づきLICを取得
S350
不一致
LIDの一致
S351
一致
S352
禁止
ACの確認
LICをKPom5にて暗号化
E(KPom5, LIC)の生成
S353
E(KPom5, LIC)をKs2bにて暗号化
E(Ks2b, E(KPom5, LIC))の生成
S354
複製
ACの確認
S355
移動
LBAに対する
有効フラグを無効に変更
S356
ログメモリの
ST1を"送信済"に変更
S357
E(Ks2b, E(KPom5, LIC))
の出力
S358
S359
E(Ks2b, E(KPom5, LIC))
の受理
E(Ks2b, E(KPom5, LIC))
の出力
S360
S361
E(Ks2b, E(KPom5, LIC))の受理
S362
E(Ks2b, E(KPom5, LIC))をKs2bにて復号
E(KPom5, LIC)の受理
E(KPom5, LIC)をKom5にて復号
LICの受理
S363
S364
LICの格納先LBAを出力
LICの格納先LBAを受理
S365
S366
ログメモリに格納先LBAを記録
S367
LIDの一致
一致
不一致
S371
エラー通知の出力
S372
エラー通知の出力
エラー通知の受理
S373
書込拒否による終了
S368
格納先LBAにLICを記録
格納先LBAに対する
有効フラグを有効に変更
S369
ログメモリの
ST1を"受信済"に変更
S370
正常終了

【図１９】


再生回路 150
コントローラ 108
HD 20
開始
S401
証明書の出力要求の出力
S402
証明書の出力要求の受理
Cp3の出力
S403
Cp3の受理
S404
Cp3の出力
S405
Cp3の受理
S406
Cp3を検証
S407
非承認
承認
KPcp3の受理
S408
Ks1dの生成
S409
KPcp3にてKs1dを暗号化
E(KPcp3, Ks1d)の生成
S410
E(KPcp3, Ks1d)の出力
S411
E(KPcp3, Ks1d)の受理
S412
E(KPcp3, Ks1d)の出力
S413
E(KPcp3, Ks1d)の受理
S414
E(KPcp3, Ks1d)をKcp3にて復号
Ks1dの受理
S415
セッション鍵Ks2dの生成
S416
Ks2dをKs1dにて暗号化
E(Ks1d, Ks2d)の生成
S417
E(Ks1d, Ks2d)の出力
S418
E(Ks1d, Ks2d)の受理
S419
E(Ks1d, Ks2d)の出力
S420
E(Ks1d, Ks2d)の受理
S421
E(Ks1d, Ks2d)をKs1dにて復号し
Ks2dの受理
S422
対象LICの格納LBAを出力
S423
対象LICの格納LBAを受理
S424
格納LBAに対する
有効フラグ
S425
無効
有効
格納LBAに基づきLICを取得
S426
再生制限
無
ACの確認
S427
再生不可
回数制限有
格納位置のACを変更
S428
KcをKs2dにて暗号化
E(Ks2d, Kc)の生成
S429
E(Ks2d, Kc)の出力
S430
E(Ks2d, Kc)の受理
S431
E(Ks2d, Kc)の出力
S432
E(Ks2d, Kc)の受理
S433
E(Ks2d, Kc)をKs2dにて復号
Kc受理
S434
正常終了
エラー通知の出力
S435
エラー通知の受理
S436
再生拒否による終了

【書類名】　　要約書

【要約】

【課題】　相当数記録されたライセンスの中から送受信処理中のライセンスを迅速に特定でき、特にライセンスの送受信処理中に異常が発生したときに、ライセンスの保護と再処理の高速化とを両立するデータ記録装置を提供する。

【解決手段】　データ記録装置としてのＨＤ（ハードディスク）２０，２１におけるコントローラ２１４は、暗号化コンテンツデータを復号するためのコンテンツ鍵などを含むライセンスをセキュアデータ記憶部２５０に記憶する。ライセンスは、セキュアデータ記憶部２５０内においてＬＢＡ（アドレス情報）によって管理され、また、送受信処理中のライセンスが格納されるＬＢＡがログとしてセキュアデータ記憶部２５０内のログメモリに格納される。そして、送受信処理中に異常が発生したときは、ログメモリに格納されたＬＢＡに基づいて送受信処理中であったライセンスが特定される。

【選択図】　　図６

出 願 人 履 歴 情 報

識別番号　〔０００００１８８９〕

１．変更年月日　１９９３年１０月２０日
［変更理由］　住所変更
住　所　大阪府守口市京阪本通２丁目５番５号
氏　名　三洋電機株式会社

出 願 人 履 歴 情 報

識別番号　〔０００００５０４９〕

１．変更年月日　１９９０年　８月２９日
［変更理由］　新規登録
住　所　大阪府大阪市阿倍野区長池町２２番２２号
氏　名　シャープ株式会社

出願人履歴情報

識別番号　〔０００００４３２９〕

１．変更年月日　１９９０年　８月　８日
［変更理由］　新規登録
住　所　神奈川県横浜市神奈川区守屋町３丁目１２番地
氏　名　日本ビクター株式会社

出 願 人 履 歴 情 報

識別番号　〔０００００５０１６〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都目黒区目黒１丁目４番１号
氏　名　パイオニア株式会社

出　願　人　履　歴　情　報

識別番号　〔０００００５１０８〕

１．変更年月日　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所

出　願　人　履　歴　情　報

識別番号　〔３００００１７６３６〕

１．変更年月日　２０００年　２月２８日
［変更理由］　新規登録
住　所　東京都新宿区新宿４－２－１８　新宿光風ビル６Ｆ
氏　名　フェニックステクノロジーズ株式会社

２．変更年月日　２００２年　４月　４日
［変更理由］　住所変更
住　所　東京都千代田区丸の内１－３－１　東京銀行協会ビル１４Ｆ
氏　名　フェニックステクノロジーズ株式会社

３．変更年月日　２００２年　８月１６日
［変更理由］　住所変更
住　所　東京都新宿区新宿４－２－１８　新宿光風ビル６Ｆ
氏　名　フェニックステクノロジーズ株式会社

４．変更年月日　２００３年　１月　８日
［変更理由］　住所変更
住　所　東京都千代田区丸の内１－３－１　東京銀行協会ビル１４Ｆ
氏　名　フェニックステクノロジーズ株式会社

出 願 人 履 歴 情 報

識別番号　〔０００００５２２３〕

１．変更年月日　１９９６年　３月２６日
［変更理由］　住所変更
住　所　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　富士通株式会社